The Parliament of the Commonwealth of Australia

# Report 400

## Review of Aviation Security in Australia

Joint Committee of Public Accounts and Audit

June 2004
Canberra

ISBN 0 642 78452 3

# Contents

Foreword ix
Membership of the Committee xi
Membership of the Sectional Committee xii
Duties of the Committee xiii
Terms of reference xv
List of abbreviations xvii
List of recommendations xxi

## REPORT

**1 Introduction 1**

**Australia's aviation security framework 1**
**Aviation under review 4**
**The Committee's inquiry 7**
**Report structure 8**

**2 Current threat environment 11**

**Introduction 11**
**Australia in the world context 12**
**Categorisation of airports 13**
Committee comment 15
**Threats facing Australia's aviation industry 15**
Terrorism threats 16

Passengers with mental health problems ........ 23

Passengers in custody ........ 23

Airport rage ........ 28

**Comparing Australia's aviation security with international benchmarks ........ 32**

**Committee conclusion ........ 34**

**3 Security enhancements ........ 37**

**Introduction ........ 37**

**Booking, ticketing, and check-in ........ 37**

Scrutiny of documents ........ 38

Passenger information ........ 39

Use of biometrics ........ 41

**Screening of passengers and air cargo ........ 48**

Current screening technologies ........ 49

Emerging screening technologies ........ 51

**In-flight security ........ 53**

Airspace modelling ........ 54

On-board security devices ........ 54

Air Security Officer program ........ 59

**Whole of government approach ........ 61**

**Limitations of technology ........ 62**

**Committee comment ........ 63**

**4 Meeting the costs of security enhancements ........ 65**

**Introduction ........ 65**

**Balancing additional costs with potential impacts ........ 66**

**Costs of increasing security at airports ........ 67**

Costs at major airports ........ 67

Costs at regional airports ........ 68

**Meeting the additional costs for security at airports ........ 70**

Major airports ........ 70

Regional airports ........ 72

**Meeting the costs of the Air Security Officer program ........ 74**

**Committee comment ........ 74**

5 Interactions between aviation participants ..... 77

Introduction ..... 77

Interactions between the regulator and the stakeholders ..... 77

Consultations concerning the legislation ..... 78

Provision of intelligence, advice, and guidance ..... 80

Interactions between aviation industry participants ..... 85

Commonwealth and State police forces ..... 85

Security committees at airports ..... 88

6 Security procedures at airports ..... 93

Introduction ..... 93

Legislated requirements ..... 94

Airport security committees ..... 94

Airport areas and security zones ..... 96

Trial of additional security procedures ..... 101

Committee comment ..... 102

Security procedures at non-regulated airports ..... 102

Committee comment ..... 103

7 Training ..... 105

Introduction ..... 105

Check-in staff ..... 106

Screening staff ..... 107

Private or public sector screening ..... 109

Committee comment ..... 109

Flight and cabin crew ..... 110

Airport ground staff ..... 111

Committee comment ..... 113

8 Auditing performance ..... 115

Introduction ..... 115

Audits undertaken by screening service contractors ..... 115

Audits undertaken by airports and airlines ..... 116

Committee comment ..... 118

**Audits undertaken by the regulator** .......... **119**

Competency of DoTaRS staff .......... 119

Training of departmental inspectors .......... 120

Types of audit performed .......... 121

Audits of airports and airlines .......... 123

Audits of air cargo operations .......... 124

Penalties for breaches .......... 125

Committee comment .......... 128

**9 Aviation security culture** .......... **131**

**Introduction** .......... **131**

**Security culture at small airports** .......... **132**

Committee comment .......... 133

**Security culture at large airports** .......... **134**

Security incident at Melbourne Airport—a case study .......... 135

Committee comment .......... 135

**Engaging the public** .......... **138**

Committee comment .......... 139

**Committee conclusion** .......... **140**

**APPENDICES**

**A Appendix A—List of Submissions** .......... **143**

**B Appendix B—List of Exhibits** .......... **147**

**C Appendix C — Witnesses appearing at the public hearing** .......... **149**

**Canberra, Thursday 4 September 2003** .......... **149**

**Canberra, Friday 5 September 2003** .......... **151**

**Sydney, Thursday 2 October 2003** .......... **152**

**Melbourne, Tuesday 12 October 2003** .......... **154**

**Brisbane, Wednesday 12 November 2003** .......... **155**

**Canberra, Monday 24 November 2003** .......... **156**

Appendix D—Inspection visits....157

**Tuesday 20 May 2003....157**

Inspection and briefing at Kingsford Smith Airport Sydney....157

**Wednesday 1 October 2003....158**

Inspection and briefing at Tamworth Airport....158

Inspection and briefing at Coffs Harbour Airport....158

# Chairman's foreword

This report presents the Joint Committee of Public Accounts and Audit's review of aviation security in Australia. The review arose from the Committee's statutory obligation to review reports of the Auditor-General, namely *Audit Report No. 26, 2002–2003, Aviation Security in Australia* which was tabled in January 2003.

Australia's aviation industry services approximately 50 million international and domestic passenger movements each year and involves some 70 000 employees who contribute in one way or another to aviation security. The industry is regulated by the Department of Transport and Regional Services.

The Committee has reviewed the current threat environment within which Australia's aviation industry operates, the opportunities and costs of security enhancements, the aviation security framework, and the human aspects of security, including the culture of security.

In summary, the security measures under which aviation security operates in Australia are appropriate to the current level of threat, there is flexibility to adjust the framework to meet changing threats, and the culture of security is positive.

The Committee has identified the security culture as being one of the more important aspects of security and is pleased with the attitude of employees at the interface between the aviation industry and the travelling public. The Committee has drawn on its own experiences of airline travel in Australia and overseas and notes the friendly, yet firm and professional attitude of the personnel involved in aviation security.

This security attitude in Australia contrasts markedly with the attitudes of security personnel, particularly screeners, in some other countries. The alternative—belligerence, heavy handedness, and arrogance—will not engage the public and will hinder security outcomes.

The Committee has made five recommendations aimed at:

- clarifying the interaction between the newly created Australian Government airport security committees and existing airport security committees;
- strengthening the regulations by the inclusion in them of the non-negotiable aspects of the security framework;
- improving the procedures for the return of expired aviation security identification cards;
- broadening security awareness training to cover everyone who has access to security-controlled areas at airports; and
- maintaining the positive security culture through the introduction of educational measures aimed at promoting a robust security culture.

Overall, the Committee is satisfied that the standard of security at Australia's airports and on aircraft is sufficient to meet the current threat environment. From time to time there will be security incidents triggered by circumstances at various layers in the system. Sometimes an incident which may appear trivial to the casual observer will cause major disruption. The Committee believes this shows aviation participants are taking their security responsibilities seriously.

I regard this report as being a positive report card for aviation security in Australia at this point in time.

**Mr Bob Charles MP**
**Chairman**

# Membership of the Committee

## 40th Parliament

**Chairman** Mr Bob Charles MP

**Deputy Chair** Ms Tanya Plibersek MP

**Members**

Senator Stephen Conroy (until 10/09/03)

Senator John Hogg (until 5/02/03, from 10/09/03)

Senator Gary Humphries (from 10/09/03)

Senator Kate Lundy (until 01/04/04)

Senator Claire Moore (from 01/04/04)

Senator Andrew Murray

Senator Nigel Scullion

Senator John Watson

Mr Steven Ciobo MP

Mr John Cobb MP

Mr Petro Georgiou MP

Ms Sharon Grierson MP

Mr Alan Griffin MP

Ms Catherine King MP

Mr Peter King MP

The Hon Alex Somlyay MP

# Membership of the Sectional Committee

| | | |
|---|---|---|
| **Chairman** | Mr Bob Charles MP | |
| **Deputy Chair** | Ms Tanya Plibersek MP | |
| **Members** | Senator John Hogg | Mr Steven Ciobo MP |
| | Senator John Watson | Mr John Cobb MP |
| | | Ms Sharon Grierson MP |
| | | Ms Catherine King MP |
| | | The Hon Alex Somlyay MP |

# Committee Secretariat

| | |
|---|---|
| **A/g Secretary** | Mr James Catchpole |
| **Inquiry Secretary** | Dr John Carter |
| **Research Officer** | Ms MaryEllen Miller |
| **Administrative Officer** | Ms Maria Miniutti |
| | Ms Jessica Butler |

# Duties of the Committee

The Joint Committee of Public Accounts and Audit is a statutory committee of the Australian Parliament, established by the *Public Accounts and Audit Committee Act 1951*.

Section 8(1) of the Act describes the Committee's duties as being to:

(a) examine the accounts of the receipts and expenditure of the Commonwealth, including the financial statements given to the Auditor-General under subsections 49(1) and 55(2) of the *Financial Management and Accountability Act 1997*;

(b) examine the financial affairs of authorities of the Commonwealth to which this Act applies and of intergovernmental bodies to which this Act applies;

(c) examine all reports of the Auditor-General (including reports of the results of performance audits) that are tabled in each House of the Parliament;

(d) report to both Houses of the Parliament, with any comment it thinks fit, on any items or matters in those accounts, statements and reports, or any circumstances connected with them, that the Committee thinks should be drawn to the attention of the Parliament;

(e) report to both Houses of the Parliament any alteration that the Committee thinks desirable in:

(i) the form of the public accounts or in the method of keeping them; or
(ii) the mode of receipt, control, issue or payment of public moneys;

(f) inquire into any question connected with the public accounts which is referred to the Committee by either House of the Parliament, and to report to that House on that question;

(g) consider:

(i) the operations of the Audit Office;
(ii) the resources of the Audit Office, including funding, staff and information technology;
(iii) reports of the Independent Auditor on operations of the Audit Office;

(h) report to both Houses of the Parliament on any matter arising out of the Committee's consideration of the matters listed in paragraph (g), or on any other matter relating to the Auditor-General's functions and powers, that the Committee considers should be drawn to the attention of the Parliament;

(i) report to both Houses of the Parliament on the performance of the Audit Office at any time;

(j) consider draft estimates for the Audit Office submitted under section 53 of the *Auditor-General Act 1997*;

(k) consider the level of fees determined by the Auditor-General under subsection 14(1) of the *Auditor-General Act 1997*;

(l) make recommendations to both Houses of Parliament, and to the Minister who administers the *Auditor-General Act 1997*, on draft estimates referred to in paragraph (j);

(m) determine the audit priorities of the Parliament and to advise the Auditor-General of those priorities;

(n) determine the audit priorities of the Parliament for audits of the Audit Office and to advise the Independent Auditor of those priorities; and

(o) undertake any other duties given to the Committee by this Act, by any other law or by Joint Standing Orders approved by both Houses of the Parliament.

# Terms of reference

As part of its statutory responsibility to examine reports from the Auditor-General, the Joint Committee of Public Accounts and Audit is expanding its review of *Audit Report No. 26, 2002-2003, Aviation Security in Australia, Department of Transport and Regional Services* to inquire and report on:

a) regulation of aviation security by the Commonwealth Department of Transport and Regional Services;

b) compliance with Commonwealth security requirements by airport operators at major and regional airports;

c) compliance with Commonwealth security requirements by airlines;

d) the impact of overseas security requirements on Australian aviation security;

e) cost imposts of security upgrades, particularly for regional airports;

f) privacy implications of greater security measures; and

g) opportunities to enhance security measures presented by current and emerging technologies.

# List of abbreviations

| | |
|---|---|
| ABS | Australian Bureau of Statistics |
| AEC | Australian Electoral Commissioner |
| AFP | Australian Federal Police |
| AISA | Australian Identity Security Alliance |
| ANAO | Australian National Audit Office |
| APAM | Australian Pacific Airports Corporation (Melbourne) |
| APP | Advance Passenger Processing |
| APS | Australian Protective Service |
| ASC | Airport Security Committee |
| ASIC | Aviation Security Identification Card |
| ASIO | Australian Security Intelligence Organisation |
| ASMs | Additional security measures |
| ASOs | Air security officers |
| ASU | Australian Services Union |
| BAA | British Airport Authority |
| BAC | Brisbane Airport Corporation |

| | |
|---|---|
| BARA | Board of Airline Representatives of Australia Inc |
| CTFR | Counter-terrorism first response |
| CSIRO | Commonwealth Scientific and Industrial Research Organisation |
| DAL | Document Alert List |
| DFAT | Department of Foreign Affairs and Trade |
| DIMIA | Department of Immigration and Multicultural and Indigenous Affairs |
| DITR | Department of Industry, Tourism and Resources |
| DoTaRS | Department of Transport and Regional Services |
| DoTRD | Department of Transport and Regional Development |
| FAAA | Flight Attendants' Association of Australia |
| HLGAS | High Level Group on Aviation Security |
| ICAO | International Civil Aviation Organisation |
| ICM | Industry Consultative Meeting |
| L-3 | L-3 Communications Security and Detection Systems |
| LHMU | Australian Liquor, Hospitality and Miscellaneous Workers Union |
| MAL | Movement Alert List |
| MANPADS | Man portable air defence systems |
| NAL | Newcastle Airport Ltd |
| OVD | Optical Variable Device |
| PICs | Persons In Custody |
| PKI | Public Key Infrastructure |
| PNR | Passenger Name Record |
| SACL | Sydney Airport Corporation Ltd |

| | |
|---|---|
| SARS | Severe Acute Respiratory Syndrome |
| SQUIDS | Superconducting Quantum Interference Devices |
| TIPs | Threat Image Projection System |

# List of recommendations

### Recommendation 1

5.63 When an Australian Government security agency committee is established at a particular airport, the Department of Transport and Regional Services should be responsible for establishing a memorandum of understanding between the Government security agency committee and the corresponding airport security committee.

### Recommendation 2

6.15 The requirement for airport security committees and other essential requirements for aviation security programs should be defined in the Aviation Transport Security Regulations 2004.

### Recommendation 3

6.33 The Department of Transport and Regional Services should set a performance standard for the return of expired aviation security identification cards (ASICs) for each card issuing body. If this standard is not met, the department should review the mechanisms for ASIC return in the issuing body's ASIC program and require change if considered necessary.

### Recommendation 4

7.41 The Department of Transport and Regional Services should require aviation participants to include in their transport security programs compulsory initial and ongoing security awareness training for airport security identification card holders who have not received security training as part of their normal duties.

### Recommendation 5

9.51 The Department of Transport and Regional Services should ensure that the security programs of aviation industry participants include educational instruments designed to promote an appropriate attitude to security and, through this, a robust security culture.

# 1

# Introduction

1.1 This chapter sets out the context for the Committee’s review of Australia’s aviation security. The framework for aviation security in Australia has been created to meet Australia’s specific needs, but is based on and is consistent with internationally agreed standards. The framework is under constant review as international and domestic circumstances change. Over recent years, reviews have been conducted by governments and by entities independent of government. This inquiry falls within the latter category.

## Australia’s aviation security framework

1.2 Australia’s aviation security framework has its origins in Annex 17 of the 1944 Convention on International Civil Aviation. The Annex, titled *Security—Safeguarding International Civil Aviation Against Acts of Unlawful Interference*, contains internationally agreed standards and recommended practices for aviation security.

1.3 The Convention is administered by the International Civil Aviation Organisation (ICAO). Australia is a founding member of ICAO and has been consistently elected to its governing council as a ‘State of chief importance in air transport’.[1]

[1] DoTaRS, *Submission No. 28*, p. 193.

1.4 While signatory states are only required to implement Annex 17 in regard to international air passenger traffic, Australia chose to apply many of the measures to domestic aviation.[2] The provisions of Annex 17 were subsequently implemented by way of the *Air Navigation Act 1920* (as amended), and in particular the *Air Navigation Regulations 1947.* Since then, the aviation security framework has been augmented through the *Air Navigation (Checked Baggage) Regulations 2000*,[3] and more recently by the *Aviation Transport Security Act 2004.*

1.5 The aviation security framework is overseen by the Department of Transport and Regional Services (DoTaRS) which:

- provides advice to government and implements Commonwealth policy;
- participates in international transport and Australian counter-terrorism forums;
- uses threat assessments and intelligence information to develop security measures for incorporation in legislation or regulations;
- sets minimum standards for operators in implementing preventative security measures;
- approves the security programs of airline and airport operators;
- monitors, tests and audits industry compliance;
- regulates to enforce where necessary the preventative security measures and standards; and
- revises security policy, measures and / or standards in the light of intelligence information, monitoring or auditing.[4]

1.6 The aviation industry operators which are regulated by DoTaRS fall into three groups:

- Airline operators—operators of air services to, from or within Australia are responsible for security of their aircraft, screening of passengers and their carry-on baggage, and security control of cargo and catering. Where operators use specified aircraft, an approved aviation security program must be in place.

[2] Auditor-General, *Audit Report No. 16, 1998–1999, Aviation Security in Australia*, Canberra, 1998, p. 11.

[3] DoTaRS, *Submission No. 28*, p. 193.

[4] DoTaRS, *Submission No. 28*, pp. 202–3.

- Airport operators—operators of security categorised airports are responsible for meeting minimum regulatory standards for airport security (including physical access, and where required the counter-terrorism first response function). While the operator is responsible for overall airport security, security for individual buildings or facilities rests with the organisation having management control of those buildings or facilities.
- Regulated agents—freight forwarders and courier companies who have agreed to operate within an approved security program are responsible for using specified equipment and procedures for preventing cargo from containing explosives or incendiary devices, preventing unlawful access to cargo, and documenting security procedures for each cargo item.[5] Regulated agents are required to apply security controls for freight exported from Australia. DoTaRS advised the Committee, however, that the security regime will be extended to cover domestic freight.[6]

1.7 Each regulated aviation operator can, and often does, contract other organisations to deliver services such as catering, cleaning, and screening of passengers and baggage. Under the framework, however, regulated operators are held accountable for the actions of their contractors and employees. There is thus a 'hierarchical chain of authority'.[7]

1.8 Following the 11 September 2001 terrorist attacks in New York and Washington, ICAO amended Annex 17 to upgrade the international standards for aviation security. The Aviation Transport Security Bill 2003 was subsequently introduced to Parliament in March 2003 in part to align Australian aviation security with these revised international standards. The Bill was also designed to:

- enhance the structure of Australia's aviation security framework;
- provide adequate flexibility to reflect the rapidly changing threat environment; and
- redevelop the framework so that the legislation and supporting regulations were more readily understood and applied by government and the aviation industry.[8]

[5] DoTaRS, *Submission No. 28*, pp. 194–5.

[6] DoTaRS, *Submission No. 79*, pp. 433–4.

[7] Auditor-General, *Audit Report No. 26, 2002–2003, Aviation Security in Australia*, Canberra, 2003, p. 10.

[8] *Aviation Transport Security Bill 2003, Explanatory Memorandum*, pp. 1, 5.

1.9 The Bill was passed by Parliament on 3 March 2004 and received Royal Assent on 10 March 2004, whereupon it took effect. At the time of this report, however, the associated regulations have yet to be promulgated.

## Aviation under review

1.10 Because of the importance of aviation to the economy and the potential impact of any security-related incident, Australia's aviation security has been subject to regular reviews.

1.11 In 1998, the Auditor-General audited the then Department of Transport and Regional Development's (DoTRD's) implementation of Annex 17 in Australia. The audit assessed DoTRD's:

- development of an appropriate risk management strategy;
- implementation of measures to ensure industry compliance with Annex 17;
- dissemination and coordination of relevant intelligence; and
- the implementation of suitable response arrangements, supported by appropriate training programs.[9]

1.12 The audit was conducted when the major security concern was criminal activity at airports.[10] DoTRD agreed with the audit report's recommendations which were designed to strengthen the regulatory regime by:

- providing a more systematic risk management strategy;
- tightening DoTRD's audit processes and follow-up actions;
- improving data collection and analysis; and
- improving DoTRD's National Training and Exercise Program.[11]

1.13 The Committee reviewed the 1998 audit report in 1999 and, in keeping with the audit's focus on criminal activity, recommended that there be a review of 'arrangements for cooperation between airport authorities and police forces in dealing with criminal activity at airports.'[12]

[9] Auditor-General, *Audit Report No. 16, 1998–1999,* p. 12.

[10] Mr Michael Lewis, *Transcript,* 4 September 2003, p. 9.

[11] Auditor-General, *Audit Report No. 26, 2002–2003,* p. 23.

[12] JCPAA, *Report 371, Review of Auditor-General's Reports 1998–99 First Half,* Canberra, September 1999, Recommendation 1, p. 9.

1.14 The outcome has been the establishment of a series of memoranda of understanding between the Australian Federal Police (AFP) and State police forces, and between the AFP and DoTaRS. As well, there are contractual agreements between the Australian Protective Service (APS) and the operators of airports where the APS has a presence.

1.15 The terrorist attacks on 11 September 2001 introduced a new dimension to aviation security. The change in the threat environment prompted a high-level government review of Australia's security and counter-terrorism arrangements.

1.16 The outcome of this review, known as the Cornall review, was announced by the then Attorney-General in December 2001. Initiatives included transferring responsibility for airport physical security and counter-terrorism first response to the Attorney-General's portfolio,[13] and the creation of Air Security Officers who became available for deployment in December 2001.[14]

1.17 The Cornall review also led to the announcement in December 2002 of changes to air passenger and baggage screening and access control.[15] These changes were:

- an increased number of airports where there was mandatory screening of passengers and their carry-on baggage;
- the introduction of the goal of ensuring cutting edge technology was used at the screening points at international and domestic airports;
- the introduction by the end of 2004 of 100 per cent checked bag screening for all international services (a year ahead of the deadline set by ICAO); and
- the introduction of checked bag screening for domestic services by the end of 2004.[16]

1.18 Meanwhile, during 2002 the Auditor-General reviewed DoTaRS' response to the heightened threat environment posed by the September 2001 terrorist attacks. The objectives of the audit also included determining the

[13] Hon Daryl Williams MP, Attorney-General, Media Release, *Upgrading Australia's Counter-Terrorism Capabilities*, 18 December 2001, p. 2.

[14] Hon Daryl Williams MP, Attorney-General, Media Release, *Air Security Officers*, 18 December 2001.

[15] DoTaRS, *Submission No. 29*, p. 192.

[16] Hon John Anderson MP, Minister for Transport and Regional Services, Media Release, *Background Paper: New Aviation Security Measures*, 11 December 2002.

extent to which DoTaRS' monitoring and compliance regime ensured that the aviation industry met its security obligations.[17]

1.19 The results of the audit were tabled in January 2003 as *Audit Report No. 26, 2002–2003, Aviation Security in Australia.* The Auditor-General found that:

- DoTaRS had responded well to the changed security threat environment following the September 2001 terrorist attacks;
- Australia's aviation regulatory framework was comprehensive with the combination of standard security measures and additional security measures providing a sound foundation for managing aviation security;
- the monitoring regime was essentially sound, but the quality of monitoring was variable;
- DoTaRS could show greater leadership and improve its response to non-compliance;
- DoTaRS could take a more strategic view of industry's performance and could better evaluate compliance by setting, monitoring and reviewing performance targets and using a wider range of strategies to encourage industry to meet those targets; and
- there had been slow progress in implementing some of the recommendations in the 1998 audit report.[18]

1.20 The Committee subsequently reviewed *Audit Report No. 26, 2002–2003* at a public hearing in May 2003.

1.21 A further review of aviation security was announced in August 2003 by the Minister for Transport and Regional Services. The review was conducted by the Secretaries Committee on National Security with the aim of ensuring that 'all aspects of the system are positioned to meet emerging threats.'[19]

1.22 The results of the review led to the announcement on 4 December 2003 of further changes to the aviation security framework. Besides administrative changes, additional aviation security measures included:

- an expansion of the regulatory regime to cover all of the 180 airports handling passengers, and operators of freight aircraft, charter flights, and private and corporate jets;

[17] Auditor-General, *Audit Report No. 26, 2002–2003,* p. 22.

[18] ANAO, *Submission No. 22,* p. 151.

[19] DoTaRS, *Submission No. 29,* p. 192.

- the implementation of comprehensive security programs and security measures based on individual airport risk assessments;
- the requirement for hardened cockpit doors on all regular passenger and charter aircraft with more than 30 seats (for non-jet regional aircraft this measure would be funded by the Government);
- the extension of the current regulatory regime for international air freight to cover domestic services;
- the trialling of new freight screening technology;
- the expansion of the Aviation Security Identification Card (ASIC) scheme to cover all staff at airports servicing passenger and freight aircraft;
- the extension of the checking process associated with the ASIC scheme to include all pilots and trainee pilots; and
- the requirement for general aviation aircraft to have anti-theft measures.

1.23 The Minister for Transport and Regional Services also announced that an additional $93 million would be spent by the Government to fund these measures. A Government grants program would also be created to assist, on a dollar for dollar basis, eligible smaller airports to implement appropriate security measures.[20]

1.24 The recent history of aviation security in Australia, therefore, is one of continuous review and adjustment to meet changes in the threat environment. While many of the adjustments have been initiated by the Executive, other reviewers such as the Auditor-General and parliamentary committees have an integral role. It is in the context of this ever-changing environment that the Committee has conducted this inquiry.

## The Committee's inquiry

1.25 The Joint Committee of Public Accounts and Audit has a statutory duty to 'examine all reports of the Auditor-General', and the powers to report to Parliament 'on any items or matters' in the Commonwealth's 'accounts, statements and reports, or any circumstances connected with them'.[21]

[20] Hon John Anderson MP, Minister for Transport and Regional Services, Media Release, *Enhanced Aviation Security Package Announced*, 4 December 2003.

[21] *Public Accounts and Audit Committee Act 1951*, Sections 8(1)(c) & (d).

1.26 The Committee reviewed the first audit report into aviation security in 1999 and reported its findings in *Report 371*. The second audit report, *Audit Report No. 26, 2002–2003*, was also reviewed by the Committee at a public hearing on 21 May 2003.

1.27 Shortly after the May 2003 hearing there were three serious aviation security incidents in Australia. These were:

- 22 May 2003—members of the public entered a secure area at Sydney airport resulting in the shutdown of a domestic terminal;
- 29 May 2003—the attempted hijack of an aircraft flying between Melbourne and Launceston; and
- 30 May 2003—unscreened passengers entered a secure area at Sydney airport resulting in the shutdown of a domestic terminal.

1.28 In light of these incidents and the heightened security environment existing in Australia, the Committee resolved on 4 June 2003 to extend its review of *Audit Report No. 26, 2002–2003*, under broadened terms of reference.

1.29 Invitations to provide submissions to the inquiry were advertised in the national press on 13 and 14 June 2003. Over 90 submissions were received—a list can be found at Appendix A. Some 13 exhibits were received—a list is at Appendix B. A number of confidential submissions and exhibits was also received.

1.30 The Committee held public hearings in Canberra, Sydney, Melbourne, and Brisbane between September and November 2003. A list of witnesses at the hearings can be found at Appendix C.

1.31 As well, the Committee inspected facilities at two regional airports—Tamworth and Coffs Harbour—which complemented an inspection of Sydney’s Kingsford-Smith Airport conducted as part of the initial review of *Audit Report No. 26, 2002–2003*. Details of the three inspections are in Appendix D.

## Report structure

1.32 This report can be seen as comprising three sections. In order, these are:

- a discussion of the current threat environment in which aviation operates in Australia (Chapter 2);
- discussions of the ‘non-human’ aspects of aviation security:

  - ⇒ the recent or potential security enhancements provided through using new or emerging technology (Chapter 3); and
  - ⇒ how the costs of these measures could be met (Chapter 4); and
- discussions of the 'human' aspects of aviation security:
  - ⇒ information sharing (Chapter 5);
  - ⇒ the rules and procedures underpinning regulation (Chapter 6);
  - ⇒ auditing compliance with those rules and procedures (Chapter 7);
  - ⇒ the training of personnel (Chapter 8); and
  - ⇒ the culture of security (Chapter 9).

1.33 A copy of this report and the public submissions received by the Committee are available on the Committee's website at http://www.aph.gov.au/house/committee/jpaa/reports.htm

# 2

# Current threat environment

## Introduction

2.1 Australia's aviation industry services approximately 50 million international and domestic passenger movements each year and involves some 70 000 employees who contribute in one way or another to the aviation security environment.[1] The contributors to the aviation security environment include:

- airlines;
- airports;
- border control agencies;
- Commonwealth and State/Territory police and protective security agencies;
- Commonwealth and State/Territory government departments; and
- intelligence agencies.[2]

2.2 Australian aviation has to operate in the world context and counter a variety of threats. The nature and intensity of these threats may vary from airport to

[1] Mr Andrew Tongue, *Transcript*, 4 September 2003, p. 12.

[2] Mr Andrew Tongue, *Transcript*, 4 September 2003, p. 12.

airport due to location and the types of aircraft and passenger services that operate. Two additional issues of importance to the Committee are the nature of the threats facing Australian aviation, and whether Australia is meeting the benchmarks set by other countries.

## Australia in the world context

2.3 The threat environment Australian aviation now faces is very different from that of three years ago. The terrorist attacks of 11 September 2001 in New York and Washington, and 12 October 2002 in Bali have dramatically altered the environment in which both international and domestic aviation industries operate. In particular, the attacks on the World Trade Centre and the Pentagon on 11 September 2001 demonstrated the potential for terrorist groups to use aircraft as weapons with potential for enormous loss of life and extensive damage. Since that event the global aviation community has existed in a state of continuing alert.

2.4 The ICAO responded to the 2001 attacks by revising the guidelines described in Annex 17 to the Chicago Convention—the document which underpins the aviation security practices of ICAO member states. As noted in Chapter 1, the international changes have impacted significantly on the aviation security requirements in Australia. Amongst other measures, passenger screening was mandated at all categorised airports in Australia.[3]

2.5 The fieldwork for *Audit Report No. 26, 2002–2003,* was undertaken in the post-11 September 2003 environment. The audit report commented that DoTaRS' response to the terrorist attacks of that day was 'rapid and appropriate'. The ANAO noted that within a few hours of learning of the attacks, DoTaRS had issued its first set of additional security measures (ASMs) to airports and airlines. Reassessment and variations to the ASMs continued frequently over the following weeks and the audit report adds that 'DoTaRS does not consider that a significant lessening of the current ASM requirements will occur for some time.'[4]

2.6 While recent changes to aviation security in Australia have largely been in response to terrorism incidents overseas, it should be remembered that terrorism is only one aspect of the threat environment in which aviation operates. As DoTaRS noted:

[3] DoTaRS, *Submission No. 79,* p. 450.

[4] Auditor-General, *Audit Report No. 26, 2002–2003,* pp. 30, 31.

> The international security environment is built on unlawful interference with aviation, of which terrorism is only a part.[5]

## Categorisation of airports

2.7 Each airport in Australia will have a unique combination of factors which contribute to its risk profile. The role of the regulator is to determine the risk profile of the airport and, based on this, determine whether or not the airport will be subject to regulation.

2.8 At the commencement of the inquiry, DoTaRS operated a system of airport categorisation that determined which airports were subject to regulation. The categorisation system was primarily based on whether or not jet aircraft used an airport. Risk assessment and traffic of passengers were additional criteria for ascertaining the level of categorisation. DoTaRS explained further:

> Categorisation is a way of focussing on the size of the airport. So it is essentially a combination of the type of traffic and the number of passengers … The intelligence tells us that the focus is jet aircraft so we have to cover all those jet aircraft carrying people.[6]

2.9 Australian airports that were subject to security regulation were categorised into 5 levels. Category 1 was the highest rating and included airports such as Sydney, Melbourne and Brisbane. These had a high volume of passengers and therefore represented the 'highest assessed risk within Australia.' Level 5 categorisation applied to smaller airports where jet aircraft might use the facility, but frequency of flights and traffic volume was very small.[7]

2.10 Only categorised airports were regulated by DoTaRS and required to have security programs. In this system, most of Australia's more than 200 airports remained uncategorised and therefore unregulated by DoTaRS. Many of these airports were significant regional airports with regular passenger transport services. The airports had been excluded from regulation because the services used turbo-prop aircraft rather than jet aircraft.

2.11 The support for the airport categorisation system, based predominantly on the type of aircraft, ranged from lukewarm to rejection:

[5] Mr Andrew Tongue, *Transcript,* 4 September 2003, p. 13.

[6] Dr Andy Turner, Mr Andrew Tongue, *Transcript,* 4 September 2003, p. 26.

[7] A full list of airports categorised at that time and their level of categorisation is at DoTaRS *Submission No. 29,* pp. 215–16.

- the Tasmanian Government generally supported the security ratings, but its own civil infrastructure review suggested a higher rating for Burnie and Devonport Airports than the rating used by DoTaRS;[8]
- the Queensland Government noted that it was unaware of any security incident which indicated a greater need for security at its regional airports, but it was happy that future categorisation would be on more of a case by case basis;[9]
- Qantas agreed with the assessment that regional aircraft operations posed less of a risk than those from major cities, but thought more could be done in the regions;[10]
- the Victorian Government considered the reasons for categorisation were sometimes unclear and cited the example of Avalon Airport which was unregulated, yet had a jet maintenance facility and was used for training the crews of Boeing 747 and Airbus jet aircraft;[11]
- the Western Australia Government said that it did not wish to challenge the risk assessments, but suggested a closer look at the trigger for the requirement for passenger screening;[12] and
- the South Australian and New South Wales Governments both advocated the extension of the security system to cover all airports.[13]

2.12 The Government announcement of 4 December 2003 has addressed the concerns about the categorisation of airports. The new system removed the 'categorisation concept' and brought under regulation 'all airports handling passengers' and 'the operators of freight aircraft, charter flights, and private and corporate jets.'[14]

2.13 Under the *Air Navigation Act 1920* and its regulations, the activities of airports and aircraft operators were relatively prescribed. The requirements of aviation participants under the new *Aviation Transport Security Act 2004* are less prescriptive, more broad ranging, and allow flexibility.

2.14 Airports and aircraft operators will be required to demonstrate the following:

[8] Tasmanian Government, *Submission No. 32,* p. 241.

[9] Mr Damien Vasta, *Transcript,* 12 November 2003, p. 43.

[10] Mr Geoffrey Askew, *Transcript,* 12 November 2003, p. 22.

[11] Victorian Government, *Submission No. 71,* p. 404.

[12] Mr Andrew Gaynor, *Transcript,* 21 October 2003, p. 58.

[13] NSW Government, *Submission No. 20,* p. 143; SA Government, *Submission No. 56,* p. 309.

[14] DoTaRS, *Submission No.79,* pp. 429, 443.

> That the participant:
>
> - is aware of their general responsibility to contribute to the maintenance of aviation security;
> - has developed an integrated, responsible and proactive approach for managing aviation security;
> - is aware of, and has the capacity to meet, the specific obligations imposed by the Act;
> - has taken into account relevant features of their operation in developing activities and strategies for managing aviation security.[15]

### Committee comment

2.15 The Committee recognises the important step DoTaRS has taken to address a potential gap in the aviation security environment. By requiring all aviation participants to operate within an approved security program, DoTaRS will be in a position to ensure the robustness of the aviation security environment in Australia.

2.16 A consequence of the changes is that the number of airports with security programs will increase from 38 to 180, with variable intensity. This will place a significant oversight burden on DoTaRS as the regulator. The Committee notes that $93 million from surplus Ansett levy funds will underpin the new regulatory system.[16]

2.17 As well, there will be an impact on smaller airports, many of which were only marginal operations. They will now be required to introduce additional security measures which will have significant cost implications. The Committee discusses the enhancements to security in Chapter 3, and how additional costs might be met in Chapter 4.

## Threats facing Australia’s aviation industry

2.18 The threats facing aviation security are many and varied. In response, authorities have to devise a single ‘catch all’ system of procedures. The ANAO defined the purpose of this system as being:

> … to deter, detect and prevent attempted acts of unlawful interference. It covers the “intentional and wilful” attempts to disrupt an aircraft or flight, for example, to sabotage an aircraft.[17]

[15] DoTaRS, *Submission No.79,* p. 454.

[16] DoTaRS, *Submission No.79,* p. 452.

[17] Auditor-General, *Audit Report No. 26, 2002–2003,* p. 19.

2.19 While the costs of security measures are immense, the cost of a single 'act of unlawful interference' can also be huge. DoTaRS has estimated the possible cost of a single event as amounting to $510 million.[18]

2.20 The Committee has received evidence on a number of threats to Australia's aviation industry which were, in order of discussion in this chapter (and not necessarily in order of importance to Australian aviation):

- terrorism threats;
- threats from passengers with mental health problems;
- threats posed by passengers travelling in custody; and
- airport rage.

## Terrorism threats

2.21 The terrorist attacks of 11 September 2001 focussed world attention on the use of fully loaded passenger jet aircraft as flying bombs. In Australia the regulatory focus, until December 2003, has also been on jet aircraft. DoTaRS commented:

> The reason for that is that the intelligence tells us that jet aircraft are the focus for attention by terrorists. That is largely because they are good media targets, they travel very fast, they have high fuel loads and they do a lot of damage.[19]

2.22 Placing global aviation terrorism in context, *Audit Report No. 26, 2002–2003* commented that 'politically motivated violence represents about five per cent of all aviation security incidents globally.'[20] DoTaRS also emphasised that terrorism was but one aspect of aviation security concern.[21]

### Terrorism incidents affecting Australian aviation

2.23 The Committee sought to ascertain whether Australian aviation had been subject to terrorism. The DoTaRS witness responded that there was 'no evidence of any terrorist related incident in Australian aviation history for as far back as I can remember.'[22] This view has been confirmed by the Australian Federal Police (AFP) in answer to a question taken on notice.[23]

[18] Auditor-General, *Audit Report No. 26, 2002–2003,* p. 19, quoting from figures provided by DoTaRS in *Aviation Security Regulations 2001—Regulation Impact Statement,* p. 11.

[19] Mr Andrew Tongue, *Transcript,* 4 September 2003, p. 18.

[20] Auditor-General, *Audit Report No. 26, 2002–2003,* p. 19.

[21] Mr Andrew Tongue, *Transcript,* 4 September 2003, p. 13.

[22] Mr Andrew Tongue, *Transcript,* 4 September 2003, p. 17.

[23] AFP, *Submission No. 58,* p. 328.

2.24 In addition, Mr Clive Williams from the Strategic and Defence Studies Centre, Australian National University, told the Committee that he did not think it likely that a group would try to hijack an aircraft in Australia.[24]

2.25 Concerns, nevertheless, have been raised in the media that:

> … a light plane from a local airport is more likely to be turned into a suicide bomb than an international jet travelling from an overseas destination.[25]

2.26 The media article cited Bankstown Airport in western Sydney as being identified as a 'prime terrorist target'. The management of Bankstown Airport dismissed the article, commenting that it had contacted all of the security agencies both State and Federal with which it had dealings and that there:

> … is no evidence to support that Bankstown was identified as a threat.[26]

2.27 Bankstown Airport added that it had a very high level of security, exceeding security requirements for an airport of its categorisation, with person-proof fences, keypad gates and regular security patrols.[27]

### The use of common items as weapons

2.28 Mr Clive Williams raised the issue of common items being used as 'weapons of opportunity'. He provided the following examples:

- bottles of duty free alcohol carried by passengers into the cabin and available at Qantas' proposed self-service bars on aircraft—the alcohol could be used as a fire accelerant, or the glass bottle as a weapon;
- bottles apparently containing water could instead contain more sinister liquids which were toxic or could be used to make a weapon; and
- metal cutlery could be used as weapons—during an air-rage incident a passenger was stabbed in the neck with a fork.[28]

2.29 The Flight Attendants' Association of Australia (FAAA) agreed in principal with the banning of bottles from aircraft. It felt, however, that this would be a difficult step, as would banning the sale of duty-free alcohol to passengers on departure. It advocated, nevertheless, the examination of bottles of liquid as a standard screening procedure.

[24] Mr Clive Williams, *Transcript*, 5 September 2003, p. 61.

[25] Sun-Herald (Sydney), *Bankstown Airport named as prime terrorist target*, 14 September 2003.

[26] Mr Kimber Ellis, *Transcript*, 2 October 2003, p. 43.

[27] Mr Kimber Ellis, *Transcript*, 2 October 2003, p. 43.

[28] Mr Clive Williams, *Submission No. 35*, p. 261–2.

2.30 Qantas responded:

> What we need to do is to look at our priorities and our priorities are to prevent terrorism, so we prevent firearms and the like from being in our aircraft. I am not sure that we enhance the process by the removal of metal knifes that will not cut butter, nailfiles or duty-free alcohol. I think the examination of liquid at a screening point, and open liquid at that, is a value added part of the process, but we really need to have that balance and that is what we need to strive for.
>
> … We do have an area in our new business class fit-out that will enable people to go and serve themselves with alcohol, but it is supervised and monitored.
>
> …We do have a responsible alcohol policy. I think people themselves are more aware of it now, too. We certainly consume more water on our aircraft than alcohol.[29]

## Other countries as a launching pad for terrorism in Australia

2.31 Notwithstanding the unlikeliness of an aviation terrorist incident originating in Australia, concerns have been raised that terrorists could take advantage of lax security at the airports of Australia’s neighbouring countries to launch attacks on Australia.[30]

2.32 Qantas advised the Committee that it had an audit team which travelled around its network undertaking security audits and assessments:

> There are a number of countries where we have been less than satisfied with the security that has been provided for our operations there. We have spoken to the organisation, whether it is the airport operator or the government agency. If we are unable to have a remedy then we will introduce our own measures. There are a number of airports around the world where we will subject Qantas passengers to secondary screening because of the substandard nature, in our belief, of the primary screening. We will subject our cargo to screening if the locally provided screening does not meet a Qantas standard.[31]

2.33 Qantas added that while it was not required to notify DoTaRS, the department was ‘certainly aware’ where these additional measures had been introduced. There were international airlines flying to Australia from

[29] Mr Geoffrey Askew, *Transcript,* 12 November 2003, p. 25.

[30] Australian Associated Press, *Terrorists could use PNG as launching pad—Anderson*, 23 March 2004.

[31] Mr Geoffrey Askew, *Transcript,* 12 November 2003, p. 16.

those airports, Qantas said, but DoTaRS would need additional resources if it was to ensure that these airlines met minimum security standards.[32]

2.34 Brisbane Airport Corporation (BAC) told the Committee that like Qantas it was aware of airlines and overseas departure points which presented a possible security risk. BAC continued:

> From a political sensitivity side, that has been addressed by government. If the aircraft has arrived and the passengers are exiting the terminal, nothing is going to happen anyway, because all they want to do is escape. The government has put in place a process where we do 100 per cent screening of all transit passengers. That caters for the good carriers and the bad carriers, the good destinations and the bad destinations. … You arrive, and there is the same standard for everybody, so no-one feels they are being punished or victimised. But we know who the good ones are and who the bad ones are.[33]

2.35 DoTaRS explained that international airlines operating into Australia had to have approved aviation security programs just like Australian carriers. There was thus a measure of control over international airlines, but this did not extend to overseas airports. DoTaRS added that it was, however, working with AusAID:

> … in the near region to assist nations to develop their capability to manage their airports. … My sense is that, in the current threat environment, looking at inbound aircraft and ensuring, if you like, a more aggressive regime is possibly one of the areas that the system will evolve to capture.[34]

2.36 The Committee notes that in the 2004–05 Budget, the Government announced three initiatives aimed at enhancing aviation security in the Asia-Pacific region:

- a two year project for regional country scoping studies to assess the border management requirements of each country, followed by workshops with the recipient countries and their border agencies;
- an independent assessment of the border management and control systems of Asia-Pacific countries to identify additional requirements for more secure border management; and

[32] Mr Geoffrey Askew, *Transcript*, 12 November 2003, p. 18.

[33] Mr Edward McPheat, *Transcript*, 12 November 2003, pp. 58–9.

[34] Mr Andrew Tongue, *Transcript*, 4 September 2003, p. 21.

- assistance of $4.7 million over four years to Asia-Pacific to improve local skills in passenger screening, access control management, and security planning.[35]

## Threats from 'man portable air defence systems'

2.37 The issue of man portable air defence systems, or MANPADS, was raised by Mr Williams. In the context of global aviation security, he told the Committee that he thought the security measures introduced after September 2001 would make hijacking more difficult, but:

> … if a terrorist group wanted to have a go at an aircraft, clearly the use of a surface-to-air missile would be an easier option or perhaps more attractive option.[36]

2.38 MANPADS are shoulder-launched anti-aircraft missiles such as Stingers and SA-18s. Several thousand missiles are available to insurgents and other non-state groups. Chemring Group told the Committee:

> General capabilities of the MANPADS are that it is portable, reliable, inexpensive and fairly easy to use—that is key. Target detection range is about six miles and engagement range is about four miles. Aircraft above 15,000 feet are considered relatively safe. Take-off and landing are the most vulnerable parts of attack. It has a very large engagement footprint,[37] and it is difficult to detect on the ground.[38]

2.39 Chemring indicated that the time from launch to impact at four miles would be about fifteen seconds.[39] The witness added that MANPADS were easy to use, but training was an issue:

> As a timeline, you have to get it out of the box, you have to put the trigger guard onto it, you have to engage the battery and then it starts the cooling process. Then you have to sight it, super elevate and fire.
>
> … if the guy has never fired one before, he does not have three or four goes. He also only has about a minute of cooling time to cool the seeker head. So he has to react fairly quickly before he fires. Training is an issue, but he only has to fire it a few times before he

[35] Budget Measures 2004–05, Budget Paper No. 2, pp. 101, 104.

[36] Mr Clive Williams, *Transcript*, 5 September 2003, p. 60.

[37] The threat area around an airport is 300 square miles or 768 square kilometres.

[38] *Exhibit 10,* Committee briefing by Chemring Group Plc/Raven Alliance, 11 February 2004, Transcript p. 2; Power Point presentation p. 12.

[39] *Exhibit 10*, Transcript p. 3.

> understands what is going on. It took me two or three goes to understand how to use it, and I had never fired one before.[40]

2.40 Possible counter-measures to MANPADS are covered in Chapter 3 when the Committee discusses possible enhancements to aviation security.

2.41 Mr Williams advised the Committee that he considered MANPADS were not a threat to aircraft in Australia.[41] DoTaRS agreed that they were not a priority issue,[42] and Customs advised there had been ‘no detections of attempts to illegally import surface to air missiles.’[43] Qantas also considered the threat in Australia is ‘almost negligible.’[44]

2.42 Notwithstanding the lack of a MANPADS threat in Australian airspace, Mr Williams considered that South-East Asia was the most likely area for an attack on Australian aircraft. Specifically, the most vulnerable country would be Thailand because it was known that MANPADS were available in Indochina.[45]

2.43 DoTaRS commented that it was in constant contact with the Australian Security Intelligence Organisation (ASIO) about the anti-aircraft missile threat. ASIO in turn was in contact with its associates in other countries. DoTaRS was similarly in constant contact with Qantas and the airline was in contact with authorities in other countries about the threat.[46]

2.44 Qantas commented that there was a realisation in Australia of the ‘importance of intelligence and the importance of the timely dissemination of that intelligence.’[47]

## Committee comment

2.45 The Committee considers that the risk of a terrorist attack is dependent on intention, capability and training. Terrorist groups might have the intention of attacking Australia, its citizens or interests. In Australia, though not necessarily overseas, the capability of such groups is believed to be limited. Marshalling capability, in the form of personnel, weapons or explosives, and subsequent training exposes terrorist groups to the attention of government intelligence agencies.

[40] *Exhibit 10*, Transcript p. 4.

[41] Mr Clive Williams, *Transcript,* 5 September 2003, p. 60.

[42] Mr Andrew Tongue, *Transcript,* 4 September 2003, p. 17.

[43] Customs, *Submission No. 60,* p. 344.

[44] Mr Geoffrey Askew, *Transcript,* 12 November 2003, p. 20.

[45] Mr Clive Williams, *Transcript,* 5 September 2003, p. 60.

[46] Mr Andrew Tongue, *Transcript,* 4 September 2003, pp. 16, 17.

[47] Mr Geoffrey Askew, *Transcript,* 12 November 2003, p. 18.

2.46 Regarding the use of light aircraft as suicide bombs, the Committee draws attention to an incident on 6 January 2002 when a teenager commandeered a Cessna light aircraft and flew it into the side of a forty-two storey skyscraper in Tampa, Florida.[48] This event shows that light aircraft pose a security risk. The size of such aircraft, however, indicates that this risk is significantly less than that posed by regular passenger transport aircraft.

2.47 The Committee notes that the enhancements to aviation security announced on 4 December 2003 require anti-theft devices to be installed in light aircraft and pilots and trainee pilots to be subject to security background checks.[49] The Committee supports this initiative.

2.48 The Committee agrees with witnesses that currently the risk of a terrorist attack on aviation in Australia is low. In this context, the Committee considers the current arrangements regarding passengers carrying bottles of water and the presence of alcohol on aircraft to be appropriate.

2.49 Australia’s international carriers may on the other hand face the threat of terrorism. In such circumstances effective security relies on intelligence gathering and timely dissemination of intelligence to international carriers. The Committee expects all players in aviation security to maintain vigilance.

2.50 The Committee is pleased that DoTaRS in conjunction with AusAID is looking to improving security in airports beyond Australia’s borders. Such improvements will reduce the ability for terrorists to use other countries and foreign airlines as a conduit for an attack on Australia. The Committee believes this is an aspect of aviation security which can easily be boosted with benefits accruing to Australia and Pacific region countries. The Committee expects this initiative to continue with the appropriate resourcing.

2.51 Terrorists have a range of potential targets. Aviation with its umbrella of security is a relatively ‘hard target’. As the 11 March 2004 attack on Madrid’s rail network showed, terrorists may prefer to direct their attentions to ‘softer’ targets.

2.52 The Committee notes reports in the media that counter-terrorism agencies have identified some 300 potential terrorist targets in New South Wales.[50] As well, a man was arrested in Sydney on 22 April 2004 on terrorist

[48] *Mystery of teen’s crash into skyscraper*, in *The Australian*, 7 January 2002.

[49] DoTaRS, *Submission No. 79*, p. 458.

[50] Australian Associated Press, *Police identify almost 300 NSW sites as potential targets*, 10 May 2004.

charges—allegedly for plotting to bomb Australia's national electricity grid.[51]

2.53 The Committee also notes that the Government has turned its attention to the security of maritime and other potential terrorist targets. This is not to sound the 'all clear' for aviation—DoTaRS has provided information from a recent ASIO publication:

> Aviation is a particular focus of al-Qa'ida. The 11 September 2001 attacks in New York and Washington were its most dramatic use of aircraft for terrorist purposes. Since the 11 September attacks, terrorist interest in attacks on the airline industry and the use of aircraft as weapons has continued unabated. … There is no doubt that al-Qa'ida will maintain its interest in aircraft as weapons and targets for terrorist attacks.[52]

## Passengers with mental health problems

2.54 The history of aviation security incidents in Australia indicates that most incidents have arisen from the activities of passengers with mental health problems. As Mr Williams said:

> I think the kind of aviation security incident that is more likely to occur in Australia is the sort of thing that we have seen over the years—which is essentially a single individual, usually mentally unbalanced or stressed, creating an incident on board an aircraft and sometimes trying to take over the aircraft.[53]

2.55 DoTaRS commented that it is difficult to predict the actions of people who have a mental health problem and are making a cry for help.[54]

2.56 The Committee agrees that currently in Australia the most likely security incident will arise from a passenger with a mental health problem. Such passengers may not be identified as having a mental illness and pass through various security procedures before their problems surface. The Committee believes that a layered system of security such as that used in Australian aviation is the only way to address this threat.

## Passengers in custody

2.57 During the course of the inquiry, the carriage of persons in custody (PICs) emerged as a major concern to airlines. PICs are passengers who for

[51] *Plot to bomb power grid*, in *The Australian*, 23 April 2004.

[52] DoTaRS, *Submission No. 79*, p. 429.

[53] Mr Clive Williams, *Transcript*, 5 September 2003, p. 61.

[54] Mr Andrew Tongue, *Transcript*, 4 September 2003, p. 25.

various reasons are being transported either between jurisdictions within Australia, or being deported or removed from the country.[55]

2.58 Both the Board of Airline Representative of Australia Inc (BARA)—the industry body representing airlines—and Qantas stated that apart from terrorist events, the carriage of PICs was the single greatest risk to operations. [56]

2.59 Qantas provided details of the scale of the issue:

> Qantas uplifted 3,092 persons in custody in 2002, of which 1,906 were escorted. Between 1 January 2003 and 30 September 2003, Qantas has uplifted 1,741 persons in custody, of which 1,065 were escorted. Qantas accepts that not all persons in custody pose a risk to its operations. The company merely seeks, however, sufficient information on all persons in custody, regardless of their status, in order to make an informed assessment as to any potential risk and thereby discharge its duty of care to its passengers and staff. The necessity for carriers to be appropriately advised by authorities of the proposed carriage of persons in custody cannot be overstated.[57]

2.60 The Commonwealth Department of Immigration and Multicultural and Indigenous Affairs (DIMIA) is the primary source of PICs transported by airlines, providing upwards of 13,000 PICs each year.[58]

2.61 Evidence on this issue was taken by the Committee before the passage of the *Aviation Transport Security Act 2004* and the completion and tabling of its associated regulations. The regulations have yet to be finalised, but the Committee has received an April 2004 draft copy of the regulations.

2.62 The *Air Navigation Regulations 1947* required those intending a PIC to be carried on an aircraft to notify the operator 'as soon as practicable; and before the person in lawful custody boards the aircraft.' The operator may refuse to allow the PIC to be carried. If agreeing, the operator must notify the pilot 'as soon as practicable before the flight' and provide:

- the name of the person in lawful custody; and
- the name of that person's escort (if any); and
- the grounds on which the person is in lawful custody.[59]

[55] *Air Navigation Regulations 1947,* Regulation 33, p. 38.

[56] BARA, *Submission No. 3,* p. 15; Mr Geoff Askew, *Transcript,* 12 November 2003, p. 9.

[57] Mr Geoff Askew, *Transcript,* 12 November 2003, p. 9.

[58] DoTaRS, *Submission No. 79,* p. 4.

[59] *Air Navigation Regulations 1947,* Regulation 33 (2), (3), (4), pp. 38–9.

2.63 The Committee received evidence that agencies regularly failed to inform carriers about the carriage of PICs. BARA's submission pointed to DIMIA as a major offender:

> Of most concern to airlines is the routine failure of DIMIA to give advance notification of 'supervised and/or monitored departures'. These PIC may have been detained in custody by DIMIA, escorted to the Customs outwards control point and then released to board the aircraft alone. In some cases these 'supervised or monitored departures' have family members residing legally in Australia and such passengers are, therefore, leaving under duress.[60]

2.64 BARA provided two examples to the Committee:

> We have had instances where paedophiles have been put up the back with the unaccompanied minors on aircraft and the airlines did not know about it because the agency did not tell them. … Another instance was a person being transported back to another country for a murder trial. …The government agency even went so far as to not book the flight for that person. They made the person book the flight themselves so that the airline was not aware that it was a person who was being escorted out of the country.[61]

2.65 BARA's submission included a list of the information that it thought should be provided to airlines. The information covered the attitude of the PIC towards custody and removal, and the PIC's medical and criminal history. BARA commented that its list was not exhaustive, but it demonstrated the range of pertinent information regarding PICs that airlines required to conduct a risk assessment. The lack of such information clearly compromised the duty of care held by the airline towards the travelling public.[62]

2.66 A supplementary submission from Qantas stated that it had 'experienced many incidents of the non-notification of the carriage of a PIC' and 'across the range of agencies there are occasions where a lack of information has caused problems.' Qantas had in fact refused the carriage of fourteen PICs in 2002 and 2003.[63]

2.67 Virgin Blue advised the Committee that it had only recently become involved in carrying PICs. It had only carried a small number, but had refused the carriage of two prisoners because of unacceptable risk.[64]

[60] BARA, *Submission No. 3,* p. 15.

[61] Mr Warren Bennett, *Transcript*, 2 October 2003, p. 51.

[62] BARA, *Submission No. 3,* p. 16.

[63] Qantas, *Submission No. 77,* p. 419.

[64] Virgin Blue, *Submission No. 78,* p. 426.

2.68 DIMIA responded to the issues raised by the airlines:

> It is the normal practice to notify a carrier when a PIC from a place of detention is to be conveyed on an aircraft. This is in part reflected in the current policy guidelines for the removal and/or deportation of persons from Australia, … which states that the air carriers should be advised when persons are deported or removed. The same practice is generally followed for supervised departures.[65]

2.69 DIMIA added that it was familiar with the concerns raised by BARA and Qantas. Little had been provided in the way of substantiation despite 'repeated requests'. While BARA's examples appeared to indicate the involvement of the department, DIMIA wrote, the circumstances surrounding the removal seemed to relate to criminal law enforcement issues and not the removal of immigration detainees. Without concrete information DIMIA was not in a position to comment further.[66]

2.70 Subsequent to DIMIA's comments, a supplementary submission from BARA provided additional details. Both examples which it had raised in testimony involved Air New Zealand and DIMIA, and occurred about 8 and 4 years ago respectively. The first case involved a PIC with a paedophile record travelling from Sydney. On the aircraft the PIC was 'the subject of a complaint by the young female passenger whom the person was sitting beside.'

2.71 The second case was a PIC in custody for a murder charge and being deported from Perth. The case had attracted 'some media interest' and DIMIA 'in an apparent attempt to disguise the person's identity from Air New Zealand, arranged for the person's travel to be booked via a travel agency in Canberra.'

2.72 In both cases the airline did not make a formal complaint but made a verbal complaint to departmental staff in Sydney and Perth.[67]

2.73 DoTaRS has acknowledged that the carriage of PICs represented a significant risk to airline operators and that airlines had experienced difficulties in obtaining sufficient information from enforcement bodies such as DIMIA. DoTaRS added that any changes to the PIC requirements would have serious implications to DIMIA. Consequently, the department had sought DIMIA's cooperation to arrive at 'a solution that satisfies aviation industry participants and other Commonwealth agencies, while

[65] DIMIA, *Submission No. 81*, p. 467.

[66] DIMIA, *Submission No. 81*, p. 469.

[67] BARA, *Submission No. 91*, pp. 546–7.

meeting the Government's security objectives and international obligations.'[68]

2.74 BARA's supplementary submission stated that 'some progress has been made recently towards resolution of the airlines' concerns.' A high level meeting of senior airline representatives, DoTaRS, and DIMIA had 'produced an agreed set of protocols to be adopted by government agencies and airlines for the transport of persons in custody.' The protocols were to provide the basis for new aviation security regulations.[69]

2.75 The Committee has reviewed the April 2004 draft of the *Aviation Transport Security Regulations 2004*. The draft regulations recognise two categories of PIC carriage—supervised departures and other departures.

2.76 A supervised departure involves the movement of unlawful non-citizens who make their own travel arrangements under the supervision of DIMIA. Information including that 'relevant to the person's safety or to aviation security' has to be provided to the aircraft operator at 'least 6 hours before the intended start of the flight.'[70]

2.77 'Other departures' can involve escorted or unescorted PICs. Agencies have to provide the aircraft operator with prescribed information 'at least 48 hours before the intended start of the flight.' The information includes the reason for the person being in custody, whether the person is dangerous, and a copy of the agency's risk assessment of the person. The operator can require additional information to be provided by the agency.[71]

2.78 For both types of departure, the aircraft's pilot must be informed that a PIC is being carried and the conditions under which the PIC is travelling.[72]

## Committee comment

2.79 The Committee agrees with the airlines that the carriage of PICs poses a significant risk. The transportation of passengers who may be in custody for criminal behaviour or who may be unwillingly deported or removed from Australia creates a situation where people under stress may take inappropriate and unsafe actions.

2.80 The Committee accepts the evidence that there have been occasions when airlines were not notified of an agency's intention to transport a PIC on an aircraft. This was a breach of the previous regulations.

[68] DoTaRS, *Submission No. 79*, p. 432.

[69] BARA, *Submission No. 91*, p. 547.

[70] Draft *Aviation Transport Security Regulations 2004*, 16 April 2004, pp. 71–2.

[71] Draft *Aviation Transport Security Regulations 2004*, 16 April 2004, pp. 72–3.

[72] Draft *Aviation Transport Security Regulations 2004*, 16 April 2004, p. 74.

2.81 The Committee notes, however, that the examples provided by BARA occurred some time ago and no other more recent specific examples have been provided.

2.82 Adherence to the regulations as well as a culture of cooperation and openness is important if airlines are to meet their duty of care obligations to the travelling public. Members of the public expect to travel in safety, secure in the knowledge that the airline is fully informed of risks and threats.

2.83 The Committee is pleased that negotiations between the airlines, DoTaRS, and DIMIA have been fruitful, and there is agreement on a new set of regulations concerning PICs which cover the provision of advance information to the carriers.

2.84 The Committee expects agencies to follow the requirements of the new regulations.

## Airport rage

2.85 The issue of 'airport rage' has been raised by the Australian Services Union (ASU) which represents employees working in the customer service, clerical, administrative, and operational and supervisory functions.[73] Airport rage can be defined as disruptive passenger behaviour occurring at airports which ranges from 'the failure to obey safety instructions to verbal harassment to physical assault directed at airline staff.'[74]

2.86 The ASU suggested the reasons for such behaviour were complex, but included:

> … the impact of alcohol, the failure of consumer expectations of air travel to coincide with reality and the vagaries of air travel including delays, overbooking, flight cancellations and baggage limitations. Most of these issues find customer service staff as the front line deliverers of bad news which precipitates anger and violence from passengers and their families and friends who accompany them. As security at airports is tightened air rage at airports will increase and it must be met with sanctions for offenders.[75]

2.87 In support of its view, the ASU provided the Committee with preliminary results of a survey of its members at 14 airports.[76] Some 317 employees

[73] Ms Linda White, *Transcript*, 21 October 2003, p. 30.

[74] ASU, *Submission No. 62*, p. 359A.

[75] ASU, *Submission No. 62*, p. 360.

[76] ASU, *Exhibit No 5, Zero air rage—Preliminary survey results, October 20, 2003.*

and ground handlers of 10 airlines had responded. The ASU summarised the results:

> 96 per cent of respondents had experienced air rage while working at the airport. … a third of those respondents said that it was almost every day, 35 per cent said once a week and 27 per cent said once a month. … Seven out of 10 agents said that they had seen a passenger being threatened by another passenger; 32 per cent had seen somebody assaulted, and there have been incidents of stalking. … [the behaviour ranged] from being chested by a passenger, having briefcases or passports thrown at you, grabbing of arms, following you to the toilet to get your ASIC … being spat at and being punched.[77]

2.88 The ASU added that the incidence of prosecutions had been low and there was a culture of non-complaint because there was an expectation that 'nobody is going to do anything about it anyway'.[78]

2.89 The ASU's submission drew the Committee's attention to legislation in the USA which provided sanctions against individuals who assaulted or interfered with the duties of air carrier employees who had security duties. The penalties ranged from a fine or imprisonment, or both. If a weapon was used in the assault, the perpetrator faced up to life imprisonment.[79]

2.90 Qantas responded by advising the Committee that the number of incidents in the three years since 2001 had constantly declined. This included on-the-ground incidents as well as in-flight incidents in both its domestic and international areas of operation. Qantas provided the following statistics:

> Between 1 January and 30 September of this year [2003] there has been a total of 239 incidents, 156 in flight and 83 on the ground, compared with 362 for 2002 and 659 for 2001—a reduction of 34 per cent and 64 per cent respectively. Of the incidents in 2003, only 30—13 in the air and 17 on the ground—were classified as violent. With a travelling population of 22½ million over the first nine months, this equates to an incident rate of one in 94,000 passengers or, for violent incidents, one in 750,000 passengers.[80]

[77] Ms Linda White, *Transcript*, 21 October 2003, pp. 29–30.

[78] Ms Linda White, *Transcript*, 21 October 2003, pp. 30, 31.

[79] ASU, *Submission No. 62*, p. 360.

[80] Mr Geoffrey Askew, *Transcript*, 12 November 2003, p. 10.

2.91 Qantas added that over the same period 'the number of passengers refused boarding or off-loaded has increased by 22 per cent and 71 per cent respectively.' (Actual numbers were not provided.)[81]

2.92 Two passenger screening companies, Chubb Security Personnel and Group 4 Securitas, told the Committee that airport rage was not a problem. Group 4 said there had only been one incident in 2003.[82] Chubb's response to the Committee's question as to whether airport rage was a significant problem was:

> Certainly not. In fact, statistics on people injured at work show much lower numbers at airports. We have a much higher proportion of women working at airports than in our general workforce, which reflects the fact that it is a very good environment in which to work.[83]

2.93 The Committee recognises that passenger screening personnel are covered by a different union to the ASU, hence the experiences of screeners may not have a bearing on the ASU's concerns. Also screeners are uniformed personnel and have a greater 'authorative presence', thereby possibly reducing the likelihood of a passenger misbehaving.

2.94 The Committee, therefore, has sought further evidence from airport managements, and State and Federal Police forces on the incidence of airport rage and whether sanctions for such behaviour are appropriate.

2.95 BAC responded that it was unable to provide specific figures, but its opinion was there had been no discernable increase or decrease in airport rage. BAC noted that traditionally the incidence of airport rage at the international terminal was low because of the attitude of travellers. At the domestic terminal, however, airport rage problems are compounded by 'the numbers of meeters, greeters and farewellers that accompany travellers.'[84]

2.96 Sydney Airport Corporation Ltd (SACL) advised the Committee that there had been 'five minor incidents' since July 2001. Three allegations involved physical assault and two involved verbal abuse. SACL added that 'anecdotally, passenger frustration appears to increase when procedures are changed.'[85]

[81] Mr Geoffrey Askew, *Transcript,* 12 November 2003, p. 10.

[82] Mr Alexander George, *Transcript,* 24 November 2003, p. 2.

[83] Mr Michael McKinnon, *Transcript,* 24 November 2003, p. 19.

[84] BAC, *Submission No. 83,* p. 526.

[85] SACL, *Submission No. 84,* p. 528.

2.97 Submissions from the State Governments of NSW, Victoria and Queensland indicated the following:

- NSW—no specific figures of airport rage were provided as it wasn't a recorded category of crime, but figures for 'offensive conduct' and 'offensive language' showed no incidents in 2001 and one in 2002; assaults for the same period were 28 and 20 respectively;[86]
- Victoria—the lack of a definition of airport rage prevented reporting the incidence or the trend over the previous three years;[87] and
- Queensland—no incidents of airport rage had been reported.[88]

2.98 The AFP provided response figures for its Australian Protective Service (APS) officers at Australia's eleven security categorised airports. The APS responded to screening point incidents when the incident had escalated beyond a point where it could be resolved by the screening staff themselves. The figures were:

- 2000—24 recorded incidents;
- 2001—28 recorded incidents;
- 2002—76 recorded incidents; and
- 2003—39 recorded incidents (thought the figures were not complete[89]).[90]

2.99 The AFP noted that the rise in incidents correlated with the September 2001 terrorist attacks which prompted the introduction of 'stricter screening practices and reporting requirements upon screening authorities which may have contributed to the increase'.[91]

2.100 Regarding the appropriateness of sanctions, BAC suggested there was 'a definite need for a review'.[92] SACL believed there should be specific legislation to empower the APS 'to deal with airport specific incidents related to inappropriate and offensive behaviour.' This would assist industry to deal with passengers who made 'improper statements or bomb threats'.[93]

[86] State Government of NSW, *Submission No. 80,* pp. 463–4.

[87] State Government of Victoria, *Submission No. 86,* p. 533.

[88] State Government of Queensland, *Submission No. 85,* p. 531.

[89] The submission was dated 17 December 2003.

[90] AFP, *Submission No. 76,* p. 416.

[91] AFP, *Submission No. 76,* p. 417.

[92] BAC, *Submission No. 83,* p. 527.

[93] SACL, *Submission No. 84,* p. 528.

2.101 The Victorian Government advised that 'air rage' was a federal offence, whereas offences committed in an airport fell within State jurisdiction. While there was no designated offence of airport rage in Victoria, the behaviour could fall within the definitions of assault, offensive behaviour or indecent language. In deciding which offences may apply, the courts would consider the conduct of the person, the likely consequences of the conduct, the circumstances, and the person's state of mind. The submission added that the 'location of these offences was not generally considered relevant, as the nature of the offence is generally the same.'[94]

### Committee comment

2.102 The evidence before the Committee is contradictory. The level of officially reported airport rage incidents is low and AFP figures indicate it is decreasing. On the other hand, the ASU considers the behaviour is a problem after survey comments from 317 members and the union suggests airport rage may be under-reported.

2.103 The Committee considers airport rage is a problem and should be an issue for airport and airline managements. The onus is on employers to provide a safe working environment. Consistent with this, management should ensure staff receive training on conflict resolution.

2.104 The Committee notes that Qantas, notwithstanding its evidence to the Committee, is reported to have installed distress alarms at its check-in counters in Melbourne. As well, more security staff had been hired to respond to airport rage and other incidents.[95]

2.105 Concerning penalties, the Committee believes that adequate sanctions are available under State legislation. Indeed, if sanctions were increased, the Committee wonders whether the desired outcome would be achieved. This is because, in an environment of alleged under-reporting, increasing penalties may induce less reporting if victims knew that offenders faced more severe consequences.

## Comparing Australia's aviation security with international benchmarks

2.106 In considering the current threat environment facing Australian aviation, the Committee has been keen to determine how Australia's aviation security compared to that of other countries.

[94] State Government of Victoria, *Submission No. 86,* p. 533.

[95] Australian Associated Press, *New Qantas security measures ahead of EBA talks,* 12 May 2004.

2.107 DoTaRS compared Australia's approach to aviation security to that of the USA, Canada and the UK. The department concluded that Australia's response to the heightened threat environment was closest to the British model. DoTaRS noted that in Australia, responsibility for security had largely remained with airlines and airports while government had taken an active support and monitoring role, 'to ensure that all appropriate resources are brought to bear.'[96]

2.108 DoTaRS told the Committee that Australia's security standards met with the stringent expectations of countries such as the USA and UK, both of whom had experienced a level of terrorism unknown within Australia:

> We are subject to international review by various interests, including both national governments and airlines … we pass all those international reviews with flying colours. If we did not, Australians would not be flying to those countries. When the US, the UK or other nations come here, our airports pass with flying colours. So, as an international benchmark, Australians can be assured that we are up there with the best in the world.[97]

2.109 The Committee asked Qantas, as an airline flying to over 30 countries, to compare Australia's level of aviation security internationally. Qantas responded:

> We have improved enormously in recent times. We are certainly at the top end of the tree. There are a lot of countries that have security that is quite visible but lacks substance. One of the strengths of the Australian regime is that it is quite thick; there are a number of layers there.[98]

2.110 The value of a layered approach to aviation security was endorsed by BARA:

> Australia adopts a layered approach to aviation security. At no stage is aviation security dependent solely on one measure or program. Unlawful interference with an aircraft is checked at multiple levels to ensure the greatest capacity to detect and obstruct a potential threat. As a result, Australia has achieved world class aviation security outcomes over many years.[99]

2.111 Turning to Australia's airports the Committee asked Sydney Airport management whether it benchmarked its security performance against

[96] Mr Andrew Tongue, *Transcript,* 4 September 2003, p. 20.

[97] Mr Andrew Tongue, *Transcript,* 4 September 2003, p. 12.

[98] Mr Geoffrey Askew, *Transcript,* 12 November 2003, p. 19.

[99] BARA, *Submission No. 3,* p. 4.

overseas international airports. SACL responded that it and DoTaRS looked at 'the experiences around the world, what other people are doing and what is working well.'[100] SACL was confident that in comparison to security at the John F Kennedy and Newark airports in the USA and London airport, Sydney airport's security was:

> … at least equivalent to what happens overseas. There are different measures in place at different airports and different regulatory regimes set up different requirements, but we would certainly match the requirements of any overseas airport given the threat level that we have here.[101]

2.112 The managers of Melbourne airport, Australian Pacific Airports Corporation (APAM), told the Committee that it had been subject to a peer review by the British Airport Authority (BAA). The review included safety as well as security.[102] APAM provided the Committee a copy of the report on a confidential basis. The Committee has reviewed this report which indicates Melbourne airport's standards are 'as good as, or better than' the other international airports audited by the BAA.

2.113 The Committee is satisfied that the standard of security at Australia's major airports is sufficient to meet the current threat environment. From time to time there will be security incidents triggered by circumstances at various layers in the system. Sometimes these incidents will cause major disruption. The Committee believes this shows aviation participants are taking security seriously—to the extent they are prepared to incur a financial cost over an incident which may appear trivial to the casual observer.[103]

## Committee conclusion

2.114 The Committee believes that the measures adopted by the regulator and aviation industry in Australia are appropriate in the current threat environment. The major feature benefiting aviation security is the layered nature of security. This 'strength in depth' provides the flexibility to increase security in stages to meet changes in the threat profile.

[100] Mr Steven Fitzgerald, *Transcript,* 2 October 2003, p. 25.

[101] Mr Ronald Elliot, *Transcript,* 2 October 2003, pp. 25–6.

[102] Ms Pamela Graham, *Transcript,* 21 October 2003, p. 16.

[103] For example, on 22 May 2003 the Qantas terminal at Sydney airport was shut down for three hours when three elderly passengers wandered into a sterile area of the terminal.

2.115 It is always possible that the threat environment in Australia may change and require more exacting security arrangements. Possible enhancements to these layers are discussed in the next chapter. The Committee recognises, however, that the level of security must be balanced with the operating viability of the industry. This was a point well-made by Qantas when it said:

> The only way [to] guarantee the security of our operations would be to ground the fleet. From the moment we decide to fly, we are in the business of risk management.[104]

[104] Mr Geoffrey Askew, *Transcript,* 12 November 2003, p. 25.

3

# Security enhancements

## Introduction

3.1 This chapter discusses opportunities to enhance aviation security provided by new or recently introduced technology and programs. Aviation uses a layered security approach and each layer of security—from passenger ticketing to aircraft in flight—can be subject to enhancement though a variety of technologies and programs.

3.2 Some forms of security technology, however, involve obtaining information about passengers or the articles they are carrying on their person or in their baggage. Sometimes personal information will be gathered or revealed which is irrelevant to security risks. The use of such technology therefore may raise issues of privacy.

3.3 Enhancing security usually incurs a cost. Chapter 4 discusses how such costs might be met.

## Booking, ticketing, and check-in

3.4 The initial layers of aviation security occur when airline tickets are booked, paid for, and when passengers present themselves for check-in. The aim of security enhancements is to identify those people who represent a security risk before they enter the secure areas of an airport. Sometimes, however, this task is attempted by identifying those who represent a **reduced risk** and therefore, by elimination, those who need to be more carefully screened.

## Scrutiny of documents

3.5 People who threaten aviation security may wish to travel with false identification documentation.

3.6 DIMIA told the Committee that customs was introducing a fraudulent travel document detection system at the border. It was a 'multi-layered system' of document examination which conducted an 'ultra-violet test and a whole series of other tests in one go.'[1] The Committee notes that the system has successfully detected four people trying to enter Australia with false passports.[2]

3.7 In addition, after the terrorism attacks of 11 September 2001 DIMIA had increased the number of airport liaison officers deployed at overseas airports. The officers were stationed at the major embarkation points for travel to Australia. Their role included checking travel documents and liaising with other countries' airport liaison officers.

3.8 DIMIA advised the Committee:

> … nearly 300 people were stopped from entering Australia from a visual look at the documents, and something like 1,500 people were stopped from moving within our region, which may have included subsequent travel to Australia.[3]

3.9 The Committee notes that in the 2002–05 Budget, an additional $19.6 million was provided to DIMIA to 'manage additional referrals arising from the fraudulent travel document detection systems introduced in 2003–04.'[4]

[1] Mr Vince McMahon, *Transcript*, 5 September 2003, p. 16.

[2] Australian Associated Press, *Reports people tried to enter Australia with fake passports*, 24 April 2004.

[3] Mr Vince McMahon, *Transcript*, 5 September 2003, p. 18.

[4] Budget Measures 2004–05, Budget Paper No. 2, p. 100.

## Passenger information

### Advance passenger processing and alert list systems

3.10 DIMIA provided the Committee with information about three systems it used to provide advanced information about passengers travelling to Australia:

- the Advance Passenger Processing (APP) system;
- the Movement Alert List (MAL); and
- the Document Alert List (DAL).

3.11 The APP system was introduced in January 2003 and provided information about passengers before they flew to Australia. DIMIA told the Committee that until New Zealand adopted the system in mid-2003 the APP system was unique to Australia.[5] The APP system allows:

- an airline to verify a passenger's authority to travel to Australia before that passenger boarded the aircraft;
- DIMIA to issue a directive to airlines to prevent the boarding of particular passengers who did not have permission to travel the Australia; and
- Australian authorities to become aware of the impending arrival of particular passengers.[6]

3.12 DIMIA told the Committee that from January 2004 the APP system had been expanded to include airline crew.[7]

3.13 The MAL database stores details about people of immigration concern to Australia. Some 235 000 people were entered on MAL because:

- they had serious criminal records;
- their presence in Australia might constitute a risk to the Australian community;
- they had been barred by migration legislation from entering Australia; or
- they were of concern to law enforcement and security agencies.[8]

[5] Mr Vincent McMahon, *Transcript,* 5 September 2003, p. 13.

[6] DIMIA, *Submission No. 30,* p. 222.

[7] Mr Vincent McMahon, *Transcript,* 5 September 2003, p. 23.

[8] DIMIA, *Submission No. 30,* p. 223.

3.14 The MAL database worked in conjunction with the DAL database which contained information on over 1.6 million documents such as lost, stolen or fraudulently altered passports.[9]

3.15 The database systems were used by DIMIA officials when visa applications were received and if granted when the information was added to departmental databases.[10] As well, the databases were interfaced with the Customs border control system.[11]

## Passenger profiling

3.16 Passenger profiling seeks to identify people posing a security risk through analysing data about them. This includes their travel related information, for example:

- the booking history of the passenger—how the reservation was made, who initiated the trip, and flight information;[12] and
- whether the person was a frequent flier (hijackers have tended not to be frequent fliers).[13]

3.17 APAM commented in its submission that it believed it was 'essential to develop an individual assessment or profiling type framework so there is not a total reliance on technology.'[14]

3.18 The Deputy Privacy Commissioner raised privacy concerns with passenger profiling. He advocated that when individuals booked their tickets they be told 'what information is going to be collected on them in the first place and how that will be used.' He added that there was also anecdotal evidence from around the world that the information being collected was 'extraordinarily broad' and not necessarily relevant to the purpose.[15]

3.19 The Deputy Privacy Commissioner added that individuals should be given the opportunity to see the information collected about them. Also, if they believed the information was incorrect, they should be able to have it amended or the file annotated to record that they disputed the accuracy of the information.[16]

[9] DIMIA, *Submission No. 30*, p. 223.

[10] DIMIA, *Submission No. 30*, p. 223.

[11] Mr Vincent McMahon, *Transcript*, 5 September 2003, p. 21.

[12] Mr Udi Bechor, ICTS Technologies, *Transcript*, 21 October 2003, pp. 64, 68.

[13] Mr Clive Williams, *Transcript*, 5 September 2003, p. 67.

[14] APAM, *Submission No. 19*, p. 135.

[15] Mr Timothy Pilgrim, *Transcript*, 2 October 2003, p. 77.

[16] Mr Timothy Pilgrim, *Transcript*, 2 October 2003, p. 80.

3.20 The Committee asked Qantas to comment on the suitability of passenger profiling. The Group General Manager, Security and Operations responded:

> … in the years ahead, profiling will be a useful tool in our armoury. I think that we will need to have a look at a form of profiling or a form of trusted traveller. But, to be truly successful, some of the privacy issues that we are concerned about today will first need to be addressed. I think that, to be truly successful, you would need access to government databases or to make it a government program. So we need to identify whether it is a positive profiling or a negative profiling—are we trying to identify those who pose no risk to us or are we trying to identify those who do pose a risk to us? I think the intellectual debate needs to be had first.[17]

3.21 The Committee agrees with Qantas that to be really effective passenger profiling would need access to information held by governments both in Australia and overseas. While information held by governments in Australia is subject to veracity checking under privacy legislation, this may not be the case for information held by governments of other countries.

3.22 The Committee concludes that sadly the ‘intellectual debate’ concerning the implications of a new technology often occurs after that technology is introduced.[18]

## Use of biometrics

3.23 The use of biometric data seeks to verify the identity of an individual through one or a number of their unique physical characteristics.[19] The characteristics would be linked to documents or an authorisation. This would enable screening personnel to check not only that the documentation and associated authority was genuine, but also that the person presenting the information was not an impostor.

3.24 The Committee received evidence on the following systems which incorporate biometric data:

- a possible new Australian passport;
- SmartGate; and

[17] Mr Geoffrey Askew, *Transcript*, 12 November 2003, p. 21.

[18] Examples include: copying technology and copyright; cloning and ethics; video mobile phones and privacy.

[19] Examples of such characteristics include: fingerprints, iris patterns, visual and thermal patterns of the face, and speech patterns.

- the ‘Trusted Traveller’ system.

3.25 The Committee also received evidence on the limitations of the technology.

## A new Australian passport

3.26 The Department of Foreign Affairs and Trade (DFAT) told the Committee that ICAO had adopted facial recognition as the international standard for biometric identifiers in passports. The incorporation of this biometric information in Australia’s passports was currently being tested.[20]

3.27 The Minister’s media release stated:

> Under the proposed system, a person’s passport photo will be used to create a detailed electronic portrait of their face. The portrait will be stored on a tamper-proof microchip inside the passport. A computer will then compare this electronic portrait to the face of the person presenting a passport at an airport.
>
> … If current research and development work in Australia is successful, biometric identifiers could be added to Australian passports in the second half of 2004 …[21]

3.28 The Committee notes that in the 2004–05 Budget, an additional $2.2 million was provided to DFAT to trial a prototype biometric passport and to ensure compatibility with equipment used in the USA. As well, $4.4 million was allocated to DIMIA ‘to establish a centralised biometric database and conduct further research on biometric capability in visa and border management.’[22]

3.29 CSIRO told the Committee that this technology could be combined with anti-counterfeiting technology such as optical variable device (OVD) technology. This technology was associated with the transparent windows in Australian bank notes. CSIRO predicted that ‘within a number of years’ it would be possible to put encrypted biometric data into OVDs.[23]

## SmartGate

3.30 SmartGate is a facial recognition system being trialled for processing Qantas international flight crew through Customs at Sydney International Airport.

[20] Mr Bryce Hutchesson, *Transcript*, 5 September 2003, p. 2.

[21] Hon Alexander Downer MP, Minister for Foreign Affairs, *Media Release, Australia leads the way on passport biometrics,* 4 June 2003

[22] Budget Measures 2004–05, Budget Paper No. 2, p. 287.

[23] Dr Robert Floyd, *Transcript,* 5 September 2003, p. 34.

3.31 Customs told the Committee that some 4 000 Qantas crew were enrolled in SmartGate and there had been over 50 000 transactions.[24] The FAAA commented that the enrolment represented ninety six per cent of Qantas long-haul cabin crew, technical crew and pilots who were using the technology 'comfortably and enthusiastically.' FAAA added:

> Facial recognition technology is our preference, because it is much less invasive. … during the recent SARS epidemic, for example, it was a factor that made us comfortable in that we did not need to touch the machine or have anyone touch us. There are significant privacy implications but, as I understand it, this facial recognition technology in the current trial does not interrogate third-party databases. Basically, it is saying that the person standing in front of the machine is the person in the passport that is being presented to the machine.[25]

3.32 In the 2004–05 Budget, the Government announced that Customs would receive $3.1 million in additional funding to expand the trial of SmartGate with the aim of 'managing future biometric passports and the projected increases in passenger numbers.'[26]

## Trusted traveller systems

3.33 The trusted traveller system seeks to identify those who do not pose a security risk so that greater resources can be devoted to the remainder. The IP@SS system developed by ICTS Technologies incorporates biometric data and passenger profiling into a smart card used by air passengers.

3.34 ICTS Technologies told the Committee that at certain airports in the USA passengers sometimes had to wait ninety minutes for a security check. One outcome of a trial of the technology due to commence in Chicago, would be the reduction of waiting times.

3.35 The Committee understands that a further trial using the technology is to commence in the USA in June 2004.[27]

3.36 Under the IP@SS system, passengers would apply for a smart cart and undergo a background check. When presenting for their next flight at the check-in they would enrol in the system. Information about the passenger would be added to the card including the passenger's flight booking

[24] Ms Gail Batman, *Transcript*, 4 September 2003, p. 35.

[25] Mr Guy Maclean, *Transcript*, 5 September 2003, p. 70.

[26] Budget Measures 2004–05, Budget Paper No. 2, p. 287.

[27] Associated Press, *US: Govt to pilot registered traveller program in June,* 18 March 2004.

history—known as their PNR (passenger name record[28]). As well, the print patterns from two fingers would be used as their biometric identifier.

3.37 Security personnel at the screening point would receive information about the passenger as the card is read—the card reader would only work when the passenger's two fingerprint patterns and the card were matched. If the information from the IP@SS computer system indicated the passenger represented a lower security risk he/she would be fast tracked for boarding. In the trial of the system at Chicago airport IP@SS card holders would use a special lane.[29]

3.38 ICTS Technologies emphasised that the card did not guarantee fast track boarding every time the passenger travelled:

> … the card will not help me if, when I come to take the next flight, the rule engine shows that there is a problem with my itinerary, PNR or other signs. So it is a benefit, but it is not a joker card … It does not mean that, once you have it, you can go and pass through and nobody will check you.[30]

3.39 Currently, a separate card would be needed for each airline, but ideally just one card would be required for all the airlines in the scheme.[31]

3.40 Privacy issues were addressed because the passenger kept their card and therefore the personal information it contained. After 24 hours the personal and flight information on the IP@SS computer system was made unreadable, unless it was needed for government investigations. After 30 days it was automatically deleted. ICTS Technologies stated that this privacy protection procedure had satisfied the Dutch government (the technology had initially been developed in conjunction with the Dutch airline KLM), and the American carrier involved in the original US trial.[32]

3.41 ICTS Technologies advised the Committee that the system was being incorporated into kiosks where passengers checked themselves in for flights. A staff member would always be in attendance at these kiosks, however, to watch for signs of nervousness indicating whether a particular passenger posed a security risk.[33]

[28] The PNR comprises the files stored in the airline's reservations and departures database. The files contain information for each journey the passenger books and can be accessed by all the entities involved in that passenger's trip—from travel agent to airline. There are about 60 possible fields and sub-fields of PNR data. Each airline has its own PNR database with its own set of fields. S3 Strategic Security Solutions, *Submission No. 88,* p. 540.

[29] Mr Udi Bechor, *Transcript,* 21 October 2003, pp. 66–7.

[30] Mr Udi Bechor, *Transcript,* 21 October 2003, p. 67.

[31] Mr Udi Bechor, *Transcript,* 21 October 2003, p. 69.

[32] Mr Udi Bechor, *Transcript,* 21 October 2003, pp. 71–2.

[33] Mr Udi Bechor, *Transcript,* 21 October 2003, p. 70.

3.42 A security enhancement for the use of biometrics in the trusted traveller system was suggested by the Australian Identity Security Alliance (AISA). The enhancement involved the enrolment of biometric information in several databases controlled by different organisations. When the biometric data needed to be checked to verify an individual's identity, the computer system would check more than one database. This provided better security because an impostor would need to have altered the information in several databases to be successful.[34]

## Limitations of biometric systems

3.43 The Committee is aware of several factors which may limit the effectiveness of biometrics in enhancing aviation security. These were:

- the security of the information;
- the nature of the biometric information to be used; and
- the difficulty and costs of enrolment.

### Security of biometric information

3.44 Biometric information has to be stored on smart cards and / or central databases. The issue is whether that information can be accessed and altered by unauthorised people.

3.45 The Committee questioned DFAT on the security of the chip to be embedded in Australia's new passports. DFAT responded:

> … the chip that we ultimately choose to put into our passport will have to have all the international certifications in relation to security requirements. … The second thing is what we call PKI—public key infrastructure—which is the ability to actually write to that chip and to access the information on that chip. Obviously a country would want to write to its own chips and would want both keys—one to write and one to access. Other countries, which of course ultimately would want to access the information on that chip at border control points, would require the access key. This raises a significant issue in terms of international security of keys and whether or not there is a need for an international repository of keys.[35]

3.46 DFAT suggested that ICAO might be the organisation holding the repository of PKI keys.[36] The witness added that DFAT's databases and

[34] Dr Ed Lewis, *Transcript*, 5 September 2003, p. 49.

[35] Mr Robert Nash, *Transcript*, 5 September 2003, p. 9.

[36] Mr Robert Nash, *Transcript*, 5 September 2003, p. 9.

transmissions were all on nationally secure networks and the levels of protection used meant that unauthorised access was not considered to be a risk.[37]

3.47 The Committee considers the issue of unauthorised access is pertinent to all technology based identification systems.

### Which biometric information should be used

3.48 CSIRO commented that collecting biometric information would not be difficult. Rather, the issue to be addressed was the type of biometric information to be collected.[38]

3.49 The Committee notes that ICAO has chosen facial recognition as the international standard for passports and ICTS Technology has chosen fingerprints as the identifier.

3.50 Both have their drawbacks.

3.51 Anecdotal evidence presented to a 2003 conference by Professor Roger Clarke indicated possible flaws in the SmartGate facial recognition system. It was alleged that SmartGate 'failed to detect two visiting Japanese officials who had, as a joke on their hosts, swapped passports.'[39]

3.52 As well, if the proposed Australian passport's facial recognition system rejected a passport, the traveller would be referred to a human official who would check the traveller against the photograph in the passport. Reports in the media of research undertaken at the University of NSW has indicated that people perform poorly at identifying unfamiliar faces from photographs.[40]

3.53 The use of fingerprint patterns by ICTS Technologies' IP@SS smart card system may introduce the risk of contact transmission of diseases such as SARS—a concern raised by the FAAA.[41]

### Difficulty and costs of enrolment

3.54 In contrast to evidence from the CSIRO that collecting biometric information would not pose difficulties, AISA stated the expense of biometric systems lay in the enrolment process:

[37] Mr Robert Nash, *Transcript*, 5 September 2003, p. 10.

[38] Dr Robert Floyd, *Transcript*, 5 September 2003, pp. 34–5.

[39] *Identity software a 'failure'* in *The Australian*, 8 September 2003.

[40] *Researcher faced with identity crisis* in *The Australian* 17 March 2004. The article refers to research being undertaken by Dr Richard Kemp.

[41] Mr Guy Maclean, *Transcript*, 5 September 2003, p. 70.

> … the expense is in the enrolment process; it is not in the device. the device you are talking about is worth cents. … As soon as humans get involved in the process, there is the labour cost—that is the expensive part. That includes in this case the enrolments. So how do you capture the biometric data simply and easily?[42]

## Committee comment

3.55 The incorporation of biometric data into documents and smart cards and its use in identity verification is clearly an emerging technology. As such, it is likely to suffer from uncertainty due to the reliability of the data being collected and the complexity of the comparisons being made by the software. Progress in computing, however, is typically rapid as computers become more powerful.

3.56 Nevertheless, it would seem prudent to the Committee that biometric identification research and development should not be directed to just one type of biometric identifier. This is in case serious flaws become apparent in the methodology associated with a particular biometric identifier. The Committee notes that the UK Government is trialling national identity cards using biometric data 'including facial and iris scans and electronic fingerprints.'[43]

3.57 The Committee believes that biometric identification, if proven reliable, has great potential as it can remove the subjectivity involved when humans are involved in recognising other humans face to face or from photographs.

3.58 During the inquiry the Committee uncovered evidence of a major security breach of security at Customs facilities at Sydney Airport. The breach involved the theft of computer servers and has been discussed by the Committee in its report on information technology security.[44] Suffice it to say that any biometric information used for identification purposes must be securely held.

3.59 The use of technology should not be seen as a substitute for other aspects of security. The Committee notes that not too long ago the adage, 'the camera never lies' was widely held. With the advent of digital imaging and manipulation this is no longer the case. The Committee cautions against adopting the belief that 'the computer never lies.'

[42] Dr Ed Lewis, *Transcript*, 5 September 2003, p. 51.

[43] Associated Press, *Britain begins trial of ID cards designed to counter terrorism*, 26 April 2004.

[44] JCPAA, *Report 399, Inquiry into the Management and Integrity of Electronic Information in the Commonwealth*, Canberra, April 2003.

3.60 The Committee notes that the introduction of systems such as the ‘trusted traveller’ program are aimed at reducing queues at passenger check-ins by expediting passage and enabling the focussing of limited screening resources. In the Australian context, passengers do not experience the queues experienced by air passengers in some other countries and there appears adequate screening resources at Australia’s major airports.

3.61 For this reason, the Committee believes there is no reason to introduce trusted traveller schemes in Australia. Caution will allow such schemes to be properly evaluated for their efficiency and effectiveness. It will also enable the privacy implications of any personal information collected by these schemes to be addressed prior to any introduction in Australia.

3.62 A further risk of such schemes was raised by DoTaRS. The Committee considers this an important consideration. The witness said:

> … we remain very cautious about anything which relies on what I might call a trusted traveller arrangement, because of the potential for sleepers. The current bad guys have demonstrated, very clearly, enormous patience.[45]

## Screening of passengers and air cargo

3.63 The second layer of security occurs when passengers and their baggage pass through screening points. The screening of air cargo also represents this second security layer.

3.64 Such screening is an indirect way of identifying people posing a security risk. As DoTaRS commented:

> From our point of view, we want anything which helps us identify the bad people rather than the bad things, because I can carry something onto an aircraft and I can assure you I am not going to use it in a nasty way. Somebody else can carry exactly the same thing onto an aircraft and use it in a very dangerous and damaging way. … But we focus on the bad **things**, because we have no effective way of identifying the bad **people**.[46]
> (emphasis added)

[45] Dr Andy Turner, *Transcript*, 24 November 2003, p. 32.

[46] Dr Andy Turner, *Transcript,* 24 November 2003, p. 33.

## Current screening technologies

### Whole article scanning

3.65 L-3 Communications Security and Detection Systems (L-3) described to the Committee the screening equipment currently in use. All used X-rays, but used distinct technologies:

- conventional machines—these provide an image like a chest X-ray which the operator had to interpret;
- dual energy machines—these provide basic explosive detection capability;
- multi-view dual energy—an enhanced version of dual energy machines; and
- CT machines—similar to hospital brain scanners, these provide slice-views of the article scanned.[47]

3.66 L-3 commented:

> The prices obviously increase with the sophistication of the machine. The top end machine can cost $US1.5 million; the cheapest machine can cost $US20 000. You get what you pay for in terms of detection.[48]

3.67 L-3 added, however, that whilst the top line machine was 'fantastic at finding explosives', its throughput was 'slow and [therefore] you need a lot of them.'[49]

### Threat Image Projection System

3.68 The Threat Image Projection system (TIPs) is a software addition to X-ray screening machines. The system allows virtual images of banned items, such as guns and knives, to be superimposed on images of items being screened.

3.69 DoTaRS advised the Committee that unless specifically exempted, screening operators had to have TIPs installed on their machines and operational when in use. DoTaRS added:

> TIPs is a training tool. It is designed to teach screeners about a variety of threats. To improve training, screener performance is

[47] Mr Mark Knox, *Transcript*, 12 November 2003, p. 4.

[48] Mr Mark Knox, *Transcript*, 12 November 2003, p. 4.

[49] Mr Mark Knox, *Transcript*, 12 November 2003, p. 8.

> monitored by supervisors and screening authority security management staff.[50]

3.70 Dr John Flexman has drawn attention to an implication of the use of TIPs—the rights of employees who find their performance being constantly assessed.[51]

3.71 During its inspection visit to Coffs Harbour regional airport, the Committee observed TIPs in operation. The Committee noted that the machine operators were keen to demonstrate their skills in identifying the threat images generated by the software.

3.72 The Committee has received no adverse comments about the use of TIPs either during its inspection visits, or in submissions and evidence at public hearings.

## Explosives trace detection

3.73 The routine use of explosives trace detection equipment to screen air passengers in Australia was introduced on 1 October 2003.

3.74 Under the procedures passengers are randomly selected for explosives trace detection screening at the screening point. SACL emphasised that passenger profiling was not involved.[52]

3.75 Group 4 Securitas told the Committee that the initial test was part of 'a number of levels in the testing process.'[53] Chubb Security Personnel explained the follow-up procedures if there was a positive reading:

> You would be retraced with the equipment, just to do a second check of the system. If you were still showing positive, then there would be a series of questions that you would be asked, to try and determine whether or not there was some legitimate reason why—for example, you mentioned fertiliser or nitro-glycerine, or you might work in a fireworks factory. ... You would go through that process and, depending on what the outcome of that interview was, you may be matched up with your checked baggage and that would also have to be searched. [54]

3.76 A significant number of people have tested positive. SACL advised the Committee that six positive readings had occurred on the first day in

[50] DoTaRS, *Submission No. 82*, p. 523.

[51] Dr John Flexman, *Submission No. 59*, p. 339.

[52] Mr Ronald Elliott, *Transcript*, 2 October 2003, p. 19.

[53] Mr Alexander George, *Transcript*, 24 November 2003, p. 6.

[54] Ms Alisa Goodyear, *Transcript*, 24 November 2003, pp. 6–7.

Sydney; Group 4 advised it had 627 positive tests. None of the positives, however, had constituted a security threat.[55]

3.77 Qantas noted that it had introduced explosive trace detection in a number of its overseas freight terminals. It added that the number of positives recorded was expected to diminish as screeners became used to the equipment. But there would always be a number of alarms as the equipment was 'very sophisticated and sensitive' and would pick up those working in the mining and farming industry.[56]

## Emerging screening technologies

### Air cargo scanning

3.78 On 4 December 2003, the Government announced there would be a field trial of new freight screening technology which had been developed by CSIRO. It was anticipated that the devices which used neutrons would be able to scan an air freight container 'in less than two minutes.'[57]

3.79 CSIRO told the Committee that a laboratory prototype had been developed which had met Customs' specifications for detecting explosives, firearms and other contraband in unit loading devices—the standard air freight container. CSIRO emphasised, however, that often there was a long period between a laboratory prototype and the use of such devices in external environments.[58]

### Full body scanning

3.80 CSIRO's submission drew attention to three full body scanning devices which are in the development stage. These used different technologies:

- backscattered X-rays;
- passive millimetre-wave imaging; and
- high-temperature superconducting quantum interference devices (SQUIDS)

3.81 Backscatter X-ray scanners are able to see through clothing because they produce an image using the X-rays reflected off the body. The body

[55] Mr Ronald Elliott, *Transcript,* 2 October 2003, p. 18; Mr Alexander George, *Transcript,* 24 November 2003, p. 6.

[56] Mr Geoffrey Askew, *Transcript,* 12 November 2003, p. 15.

[57] DoTaRS, *Submission No. 79,* p. 447.

[58] Dr Warren King, *Transcript,* 5 September 2003, pp. 33–4.

appears as a grey image, but denser objects such as plastics, metals and explosives show up as dark and defined objects.

3.82 Passive imaging systems use the radiation given off by all objects. The technology relies on the difference in temperature between the body and any concealed object. The technology had a significant price and weight advantage over other systems which could enable the development of hand-held, portable imaging devices.

3.83 SQUIDS are magnetic field detectors which are extremely sensitive and measure all three axes of magnetic fields. This allows the detection of the small objects which are difficult to detect with the magnetic scanning technology currently in use.[59]

3.84 CSIRO told the Committee that the levels of radiation exposure from backscatter X-ray devices was 'far less than the radiation you are exposed to in the kitchen' and that there was 'a greater degree of exposure associated with the flight than with the scanning.' Passive imaging systems on the other hand involved no radiation exposure.[60]

3.85 Backscatter x-ray and passive imaging devices raise privacy implications because they see through clothing and produce an image of the body. CSIRO commented:

> … you cannot imagine that such technology would be brought into place without huge numbers of safeguards that would go along with the privacy issues. But, in the first instance, one can see some simplistic ways that you could do that. Sensitive areas could be removed automatically from images, et cetera, so that you could still have some capability whilst trying to avoid the worst aspects of the privacy issue.[61]

3.86 On the other hand, Adelaide Airport advocated that such devices 'should not be overlooked because of invasion of privacy'. It commented that:

> … when it comes to the crunch, if the threat exists then the use of relevant technologies to remove or reduce that threat should be able to be justified.[62]

3.87 Dr Flexman agreed with the privacy solution offered by CSIRO, but was concerned the problem had not been identified earlier:

[59] CSIRO, *Submission No. 8*, pp. 44–5.

[60] Dr Robert Floyd, Dr Stephen Guigni, Dr Warren King, *Transcript*, 5 September 2003, pp. 37–8.

[61] Dr Warren King, *Transcript*, 5 September 2003, p. 35.

[62] Adelaide Airport, *Submission No. 18*, p. 122–3.

> What is perhaps surprising is that these questions where not identified and addressed earlier on in the development of these technologies. I think this demonstrates that the security experts of tomorrow need training not only in their area of specialization but also in law, ethics and politics involved in applying any intrusive technology.[63]

3.88 The Committee notes that this is another example of the technology preceding the debate.

### Chemical and biological sensors

3.89 CSIRO's submission also commented on its work in the development of sensors for the detection of chemical and biological contaminants. The submission suggested these sensors could be integrated into the air handling systems within aircraft and airport terminal buildings.

3.90 In addition, CSIRO had been working on a 'low pressure plasma device' for destroying microbiological material in building air conditioning systems. CSIRO suggested this technology 'might be able to be modified for application in aircraft.'[64]

3.91 The Committee questions whether the development of chemical sensors would have an application for aircraft security. The range of potential chemical poisons is immense, with even those of low toxicity likely to have an effect in the confines of an aircraft cabin.

3.92 The ability to detect and destroy microbiological contaminants on board aircraft, on the other hand, may have application beyond aviation security. The recent outbreak of severe acute respiratory syndrome (SARS) drew attention to the world-wide transmission of the virus through the movement of international airline passengers. Airlines might consider installing such air sterilisation devices to aircraft to maintain their international aviation market share in the event of a pandemic.

## In-flight security

3.93 The Committee has received evidence on three aspects of enhancements or potential enhancement to in-flight security:

- airspace modelling;

[63] Dr John Flexman, *Submission No. 59,* p. 339.

[64] CSIRO, *Submission No. 9,* p. 45.

- on-board security devices; and
- the Air Security Officer Program.

## Airspace modelling

3.94 Airspace modelling enables the tracking of aircraft movements against expected flight paths. Aircraft deviating from the expected attract attention and become the focus of a possible response from authorities.

3.95 CSIRO's submission noted that currently authorities were unaware of the precise location of about half of the aircraft flying in Australia at any one time. An approach would be to install on all aircraft 'high speed avionic data links for ship-to-ship and ship-to-ground communications.' The design complexity of the system for modelling aircraft position, however, would increase dramatically with the number of aircraft involved.[65]

3.96 CSIRO's witnesses were optimistic about progress:

> The problem of knowing where aircraft are, from a technological point of view, is far less than what is was a decade ago. That is an important point. Once you know where the aircraft are, then you can start to think about the intent of an aircraft. Is it behaving in a regular pattern? Is it identifiable as a regular flight between Sydney and Melbourne, or has it gone outside of its clearance parameters?[66]

3.97 The Committee agrees with CSIRO's concern and supports any cost-effective moves to address the problem.

## On-board security devices

3.98 The Committee has received evidence on various technologies designed to be installed on aircraft to enhance in-flight security. The devices fall into two categories:

- those designed to enhance cockpit and cabin security; and
- anti-aircraft missile countermeasures.

### Cockpit and cabin security

3.99 The submission from AACE Worldwide advocated that:

[65] CSIRO, *Submission No. 8,* p. 44.

[66] Dr Neale Fulton, *Transcript*, 5 September 2003, p. 38.

> … Australia should follow the policy lead of the US and ICAO and immediately mandate the strengthening of cockpit doors, together with the provision of video surveillance and wireless threat notification … [67]

3.100 AACE Worldwide told the Committee that the secure cockpit doors contained 'Kevlar and aluminium and all sorts of security features in them to stop bullets'. Airlines were reluctant to install such doors because of retro-fitting costs which were between $US 30 000 and $US50 000 per aircraft. The cost, however, for incorporating the doors into aircraft on the assembly line was nearer to $US10 000.[68]

3.101 The wireless threat notification device envisioned by AACE Worldwide comprised a fob key about the same size as a car key. It would have a recessed button to prevent accidental activation, and would provide a silent alarm to alert the flight crew. If video surveillance cameras were installed, the flight crew could ascertain the problem and take appropriate action. The fob key device was better than the current phone arrangement because:

> … it is a lot harder for the potential hijackers to survey and keep track of all movements of all the cabin crew. Also, phones are only every 20 metres in a plane.[69]

3.102 The Committee notes that after AACE Worldwide's submission, the Government adopted the ICAO standard. This required the fitting of secure cockpit doors to all passenger aircraft carrying more than 60 people by 1 November 2003.[70] The April 2004 draft regulations require the cockpit doors to be:

- capable of resisting penetration by small-arms fire or grenade shrapnel; and
- capable of being locked and unlocked from either pilot's seat.[71]

3.103 DoTaRS subsequently advised a Senate committee that Qantas had complied with the requirement to fit secure cockpit doors, but the deadline had been extended to March 2004 for Virgin Blue. This was because Virgin Blue was unable to obtain sufficient hardened cockpit

[67] AACE Worldwide, *Submission No. 1*, p. 2.

[68] Mr Peter Reid, *Transcript*, 21 October 2003, p. 43.

[69] Mr Peter Reid, *Transcript*, 21 October 2003, pp. 46–7.

[70] AACE Worldwide's submission was dated 10 June 2003; airlines were advised of the Government's requirements for cockpit doors in early July 2003.

[71] April 2004 draft *Aviation Transport Security Regulations 2004*, p. 66.

doors from suppliers. In the meantime alternative arrangements were permitted such as locking the door or having additional staff on board.[72]

3.104 The Committee asked DoTaRS whether it was satisfied with Virgin Blue's efforts. The department responded that it was satisfied.[73]

3.105 The Committee notes that the Government's enhanced aviation security measures announced on 4 December 2003 require the fitting of hardened cockpit doors to all non-jet regional commercial and charter aircraft with a seating capacity of 30 or more.[74] The measure was to be funded by the Government.[75]

3.106 Regarding video surveillance equipment, DoTaRS commented that ICAO had yet to come to a conclusion on the issue. The department had therefore decided that peepholes would 'suffice as an appropriate surveillance mechanism' because of the costs of installing video surveillance devices.[76]

3.107 Nevertheless, Qantas advised the Committee that it had decided to install video surveillance equipment outside the cockpit doors of its aircraft.[77] On the other hand, Virgin Blue stated there were some technical issues relating to the devices. It also had practical concerns with installing video surveillance. While flight crew were directed not to open hardened doors whilst in-flight, they 'may observe a particular incident on board which may entice them to open the reinforced door … to would-be terrorists.'[78]

3.108 Qantas did not support the use of wireless threat devices. Its reasons were:

- the existing protocols were sufficient;
- inadvertent activation would be inevitable and, because there was no way flight crew could confirm whether the threat was real, the aircraft would divert to the nearest safe airport;
- unless approved by aircraft manufacturers, there was potential for electromagnetic interference with aircraft equipment;

[72] Senate Rural and Regional Affairs and Transport Legislation Committee, *Transcript 4 November 2003*, pp. 66–7.

[73] DoTaRS, *Submission No. 79*, p. 436.

[74] These aircraft do not fall within the category of 'large aircraft' referred to in the April 2004 draft of the Regulations.

[75] DoTaRS, *Submission No. 79*, p. 436.

[76] DoTaRS, *Submission No. 79*, p. 436.

[77] Qantas, *Submission No. 77*, p. 419.

[78] Virgin Blue, *Submission No. 78*, p. 426.

- once the existence of wireless threat devices became known, it would be easy for someone to obtain a device emitting on the same frequency in order to disrupt a flight;
- sufficient mitigation was provided by the hardened cockpit door and future installation of video surveillance equipment; and
- 'the logistics of controlling the distribution, return and replacement of lost devices would be enormous.'[79]

## Anti-aircraft missile countermeasures

3.109 The threat posed by MANPADS has been discussed in Chapter 2. The Committee has received evidence from the Chemring Group / Raven Alliance on countermeasures which could be deployed on aircraft to meet such a threat.

### Hardening the aircraft

3.110 Aircraft can be hardened so that they resist the impact and explosion of a missile. Examples include strengthening the airframe, protecting the control systems, and reducing the flammability of the fuel. All measures have drawbacks such as reducing the operating range of the aircraft and fuel capability.[80]

### Flare systems

3.111 Flares are released by aircraft to act as decoys to heat-seeking missiles. The advantages of such systems are:

- they are a mature technology, so proven;
- they cost about $20 per decoy and $1 million per aircraft (the system would include missile approach warning systems); and
- the decoys can be released pre-emptively during landing and take off.

3.112 The drawbacks of such systems are:

- the carriage life of the flares would need to be increased from the current 20 hours for military aircraft to 3 000 hours for civilian aircraft:
- the 2 000 degrees Celsius and burning time of the flares creates the problem of ground fires (although lower temperature flares are entering operation and the burn time can be reduced);

[79] Qantas, *Submission No. 77*, p. 420.

[80] *Exhibit No. 11*, Chemring Group / Raven Alliance, Committee briefing, 11 February 2004, *Transcript* p. 5; *Power Point presentation*, p. 14.

- the systems are only effective against the older MANPADS such as the Stinger and SA-7s. (These types are the ones currently most likely to be available to terrorist groups.)[81]

### Electronic jamming systems

3.113 The latest technology entering service with the military is the ‘laser directed IR countermeasures system’. This electronically jams the missile, disrupting flight, which triggers self destruction. The drawbacks of the system are:

- it cannot be used pre-emptively and requires an effective missile approach warning system;
- the cost is estimated to be $1 million to $3 million per aircraft (three jammers are required for a Boeing 747);
- it is still only effective against earlier MANPADS;
- it may not be effective against a multi-missile attack; and
- the equipment may create additional drag for the aircraft.[82]

### Conclusion

3.114 Chemring Group / Raven Alliance emphasised that:

- the threat from MANPADS had to be addressed by a holistic approach, which included arms control;
- transferring systems from aircraft to aircraft as schedules took aircraft to known areas of threat was inconvenient because it would take about three days to install and test the system; and
- incorporating countermeasures ability into the design of aircraft would significantly reduce costs.[83]

3.115 The Committee notes that the US Department of Homeland Security has initiated a program whereby industry is competing to provide cost-effective civilian aircraft defence systems against SA-7 to SA-18 missiles. If such a program is successful the question becomes: Will the USA impose the solution on international airlines?[84]

3.116 In addition, a bill was introduced in the US Congress in March 2004 aimed at the MANPADS problem. Provisions included encouraging:

[81] *Exhibit No. 11, Transcript,* pp. 5–6.

[82] *Exhibit No. 11, Transcript,* p. 6; *Power Point presentation*, p. 37.

[83] *Exhibit No. 11, Transcript,* pp. 9, 10.

[84] *Exhibit No. 11, Transcript,* pp. 7, 8.

- the pursuit of international treaties and agreements to limit the proliferation of MANPADS;
- expediting the certification of missile defence systems; and
- the continuance of programs to buy back MANPADS.[85]

3.117 The Committee notes a media report that Israel was testing an anti-missile system to protect its national airline, and the Singapore Government had announced that anti-missile systems would be deployed by its national airline 'in two years'.[86]

## Air Security Officer program

3.118 Air security officers (ASOs), often called 'sky marshals', are government sponsored security officers who travel covertly on aircraft. These officers may be armed. Currently, 24 countries have an air security officer program in place.[87]

3.119 The Australian air security program for Australian domestic flights commenced on 31 December 2001. When fully implemented, the program will comprise some 110 armed ASOs.[88]

3.120 In December 2003, following a reciprocal agreement between the Australian and Singaporean Governments, ASOs commenced deployment on flights between the two countries.[89] In May 2004 the program was extended to cover flights between Australia and the USA. Negotiations are also under way to further extend the program to flights between Australia and other countries including the Canada, Indonesia and New Zealand.[90]

3.121 The costs of the flight tickets provided for the ASOs in Australia is borne by the airlines. The submission from Qantas stated that the cost to date amounted to $5.4 million. If the program, however, was extended to international flights Qantas estimated the annual cost of forgone tickets would be $20 million.[91] (This issue is discussed further in Chapter 4.)

[85] CNN Wire Service, *Bill aims to speed airline missile protection,* 30 March 2004.

[86] Agence France Press, *US House panel backs anti-missile system for civil aircraft,* 30 April 2004.

[87] Ms Audrey Fagan, *Transcript,* 4 September 2003, p. 44.

[88] Minister for Justice and Customs, Media Release, *Air Security Officers take off,* 31 December 2001.

[89] Minister for Justice and Customs, Media Release, *Australian air marshals doing a great job in keeping the skies safe,* 30 December 2003.

[90] Australian Associated Press, *Deal signed for armed sky marshals aboard Aust–US flights,* 8 May 2004.

[91] Qantas, *Submission No. 17,* pp. 114–15.

3.122 The 2004–05 Budget provided an additional $15.7 million over four years to the AFP to allow the expansion of the ASO program to international destinations.[92]

3.123 Several concerns have been raised about Australia's ASO program:

- the ability of flight crew to refuse the presence of ASOs;
- the risks associated with the carriage of weapons by ASOs; and
- the implications of the ASO program for overall aviation security.

## The captain's right to refuse to carry air security officers

3.124 Mr Clive Williams commented that the captains of civilian aircraft are not bound to accept ASOs on their flights. He quickly added, however, he was unaware of such an event happening.[93]

3.125 A submission from the Australian Federal Police (AFP) advised that the relationship between pilots and the ASOs was covered 'in several annexes to the *Chicago Convention 1944* and the *Tokyo Convention 1963.'* The basic principle was that while the aircraft was in flight, the 'pilot [had] the ultimate responsibility for the operation and safety for the aircraft.'[94]

3.126 The submission noted that at the commencement of the ASO program there had been a 'small number of refusals by aircraft captains to carry ASOs'. Since agreement between the airlines and the Government on the carriage of ASOs had been reached, however, 'no refusals have been reported.' [95]

## Risks associated with the arming of air security officers

3.127 AACE Worldwide told the Committee that armed ASOs were a safety hazard because their weapons could cause decompression in an aircraft 'which probably has a higher risk of causing problems than hijackers'.[96]

3.128 The Committee tested this assertion with a witness from ToLife Technologies who had been 'the director of security in charge of all Israeli civil aviation, passengers and cargo security in Israel and overseas between 1998 and 2002.'[97]

[92] Budget Measures 2004–05, Budget Paper No. 2, p. 97.

[93] Mr Clive Williams, *Transcript,* 5 September 2003, pp. 64–5.

[94] AFP, *Submission No. 90,* p. 545.

[95] AFP, *Submission No. 90,* p. 545.

[96] Mr Peter Reid, *Transcript,* 21 October 2003, p. 47.

[97] *Transcript,* 21 October 2003, p. 80.

3.129 The witness told the Committee that security officers were on all Israeli commercial flights and carried nine millimetre Glock handguns. He was confident that a stray bullet would not cause decompression in the aircraft—it had been checked and 'certified by the safety organisation in Israel.'[98]

3.130 The Committee believes that the training of Australian ASOs is of a sufficiently high standard to ensure the appropriate response in a security incident and that the use of their firearm would not compromise the safety of the aircraft.

3.131 The Committee notes that the use of the Taser stun gun is being considered for the ASO program.[99]

## The implications of the Air Security Officer program

3.132 The use of air marshals has been criticised because of the message it sent about airport ground security. A global aviation expert has been reported as saying:

> The provision of sky marshals on board aircraft is nothing more than a tacit agreement that security on the ground, despite the many millions of dollars we spend … is simply not working
>
> … it is incumbent upon all governments to look at security again and look at the new technologies that are out there and are ready to be deployed.[100]

3.133 The Committee does not agree with this view. Rather, the deployment of ASOs is an example of a layered security approach. This system recognises that each layer has a small risk of being breached, but the overall risk will be significantly reduced as the number of layers increases.

3.134 Moreover, the history of aviation incidents in Australia, discussed in Chapter 2, has shown that to date it has been passengers with mental health problems who have caused problems. Such problems are more likely to surface during times of stress—for air passengers this probably would be during flight. The Committee concludes it is good risk management practice to have a security presence on board aircraft.

[98] Mr Moti Meital, *Transcript,* 21 October 2003, pp. 79–80.

[99] Sunday Herald Sun, *Air marshals train to stun terrorists,* 4 January 2004.

[100] Australian Associated Press, *Air marshals won't prevent terrorism—expert,* 29 January 2004.

## Whole of government approach

3.135 AISA commented that the security systems available at airports were deficient because they were 'not integrated into a total system that has secured all points in the linkage.'[101] AISA suggested that the National Security Division of the Department of Prime Minister and Cabinet could undertake the role of cross-agency coordination because it was in a position to 'coordinate DoTaRS with DIMIA, with [Customs] and so on.'[102]

3.136 Dr Flexman also believed there needed to be a way for strategic issues to be considered. He suggested the creation of a panel of experts drawn from a wide range of fields including DoTaRS. The role of the panel would be:

> … to evaluate the best choices for different airport environments and to review their choices on a regular basis. Being mindful that the best solution today may not look so attractive in say five or ten years time with the likely entry of several new and valuable technologies on to the market … Some of the tasks of this committee might be to consider: a) effective standards and means of regulating them, b) the ethics and politics, c) the cost, d) the inconvenience, e) the practicality and f) the effectiveness.[103]

3.137 DoTaRS responded by drawing attention to the creation in May 2003 of the High Level Group on Aviation Security which provided a forum 'for consultation and exchange of ideas on aviation security' between key government agencies and the aviation industry. There was also the Industry Consultative Meeting (ICM) group which comprised representatives from airlines, airports and government agencies. The ICM also had technical subgroups including one examining technological advances. DoTaRS noted that the various groups were able to call for expert assistance from various fields where appropriate.[104]

## Limitations of technology

3.138 A significant proportion of the costs of aviation security is borne by the airport operators. Consequently, they would bear the costs if they installed a technology which was found subsequently to be inadequate.

[101] Dr Edward Lewis, *Transcript,* 5 September 2003, p. 52.

[102] Dr Edward Lewis, *Transcript,* 5 September 2003, p. 53.

[103] Dr John Flexman, *Submission No. 59,* p. 340.

[104] DoTaRS, *Submission No. 89,* p. 542.

3.139 The operators of both Sydney and Melbourne airports have cautioned against a disproportionate reliance on technology.

3.140 SACL made two points in its submission, that:

- 'no technology can or will provide 100% coverage against security threats,' and
- 'all emerging technologies are expensive.'[105]

3.141 APAM did not want Australia to become 'the guinea pig for new unproven technology.' It added that the performance of many technologies had been over-emphasised:

> [The] performance claims by manufacturers can be very difficult to substantiate. In addition there are very long lead times in the development of equipment to full operational levels, ie levels where the equipment operates robustly and copes with capacity and demand.[106]

## Committee comment

3.142 The Committee has neither the technical expertise nor the technical information before it to evaluate the cost-effectiveness of particular technologies. Evidence from the airport operators SACL and APAM suggests a note of caution. The Committee agrees with this view.

3.143 The Committee concludes that an over reliance on technological solutions to guarantee aviation security is fraught with risks. In Chapter 5 and following chapters, the Committee turns to the human aspects of aviation security, including communication between aviation stakeholders, training, and the aviation security culture. The Committee believes that these human aspects are as equally if not more important as the technology deployed to ensure security.

[105] SACL, *Submission No. 15*, p. 91.

[106] APAM, *Submission No. 19*, pp. 129, 135.

# 4

# Meeting the costs of security enhancements

## Introduction

4.1 In the previous chapter the Committee discussed various aviation security enhancements and noted some of the costs associated with those enhancements. The Government as regulator of Australia's aviation industry has the power to mandate additional security measures. If additional security measures are required, the issue becomes: How are the additional costs to be met?

4.2 The aviation industry is predominantly a private sector industry hence costs can be met from operating surpluses, from shareholders, or from the travelling public through increased fares and charges. A complicating factor, however, is that many regional airports are operated by local councils—albeit on a commercial basis.

4.3 On the other hand, there is a degree of 'public benefit' arising from the industry, for example through the facilitation of tourism. Consequently, it may be argued that the general community should pay for increased security through funds provided by the Government.

4.4 In Chapter 1, the Committee observed that the aviation security environment was continually changing as circumstances changed. The Committee has received much argument as to how the costs of security enhancements should be met. This evidence, however, was received before the Government announced its enhanced aviation security package on 4 December 2003, and before the 2004–05 Budget. Both the package and the Budget provided extra funds to the aviation industry to meet increases in aviation security.

## Balancing additional costs with potential impacts

4.5 The Committee agrees with CSIRO's view that achieving total safety, if that were indeed possible, would be prohibitively expensive. CSIRO stated:

> … the cost to implement extensive systems that could potentially guarantee total safety are beyond the financial resources of the travelling public and governments, as well as a significant impediment to the use of the service and an excessive response to the estimated risk.[1]

4.6 On the other hand, the costs of security enhancements can be small relative to the loss of an aircraft, the death of passengers and consequent litigation,[2] and the impact on the economy.

4.7 This view was confirmed by Virgin Blue which told the Committee:

> I think that any incident to any airline within Australia would have catastrophic effects not only for Virgin Blue but also for Qantas, Alliance, Rex and any other airline in Australia; every airport; the hospitality industry; and the tourism industry. It would be phenomenal.[3]

4.8 Brisbane airport quantified the effect on a major airport when it told the Committee that the immediate cost of a two week shut down due to a terrorism incident was about $7 million. There would also be the ongoing costs of reduced air travel.[4]

4.9 The effect on tourism was described by the Department of Industry, Tourism and Resources (DITR). The department told the Committee that in 2002, 99 per cent of the 4.8 million international tourists travelled to Australia by air. The tourism industry contributed 4.5 per cent to the gross

[1] CSIRO, *Submission No. 9*, pp. 42–3.

[2] Mr Clive Williams, *Transcript*, 5 September 2003, p. 59.

[3] Mr Philip Scanlon, *Transcript*, 12 November 2003, p. 37.

[4] Mr Stephen Goodwin, *Transcript*, 12 November 2003, p. 54.

domestic product and employed 6 per cent of the work force. It also provided 11 per cent of Australia's total exports.[5]

4.10 DITR added:

> Following [the terrorist attack of 11 September 2001], there was a very major impact. It is somewhat difficult to disentangle that impact from the collapse of Ansett, which happened on 14 September, but into September 2001 arrivals fell by 9.1 per cent, in October by 11.3 per cent and in November by 18.2 per cent. It is also important to note that the forecasts of tourism growth prior to the September 11 events had been around 7 per cent a year over the next 10 years. Those have now been revised down to 4.6 per cent a year.[6]

4.11 There is therefore an incentive to all stakeholders in the aviation industry—from private enterprise through to government—to have the appropriate level of security commensurate with the risks. Consequently, it is reasonable for stakeholders to contribute to increased security.

4.12 There is also the argument that in a market economy those directly benefiting from aviation should make the greatest contribution. This would include the travelling public who would pay through increased fares.

## Costs of increasing security at airports

4.13 Airports can be divided into two major groups—major airports servicing mainly the capital cities and regional airports. The differences between the groups stem from the numbers of passengers passing through the airport which impacts on airport viability. This viability has led in some cases to the airport operators becoming significant private enterprise entities.

4.14 In the discussion that follows the Committee has included the screening operations of airlines with those of the airport operators.

### Costs at major airports

4.15 The cost of security at Australia's major airports is substantial. SACL told the Committee that security comprised 20%, or $28 million, of its

[5] Ms Patricia Kelly, *Transcript*, 5 September 2003, p. 25.

[6] Ms Patricia Kelly, *Transcript*, 5 September 2003, p. 25.

operating costs. Over $50 million was invested in security infrastructure. SACL added that the recently introduced explosive trace detection technology had meant an investment of an additional $1 million, with $2 million being added to annual operating costs. SACL predicted that the introduction of 'checked baggage ' screening would require a doubling of investment in aviation security which translated to spending some $80 million. This amount excluded the separate investment Qantas would have to make in its leased terminal.[7]

4.16 For Melbourne Airport, 15–20% of the budget was spent on security. APAM commented that much of its security costs were passed on to the aviation industry and ultimately to passengers.[8] A similar percentage—some 21% of total cost base—was spent by Brisbane Airport on its mandated security.[9]

4.17 For a small international airport such as Cairns the introduction of 'checked baggage' screening is predicted to cost $12–14 million to introduce. Cairns Port Authority told the Committee that when looking to recoup the cost over the ten year operating life of the equipment, the issue was the disproportionate cost which would be borne by passengers. This was because of the relatively small numbers of passengers when compared to larger international airports. The outcome was that Cairns as a destination was placed at a competitive disadvantage.[10]

4.18 The submission from Qantas stated that its security expenditure had increased by 68% in real terms since 11 September 2001. This included:

- over $2 million biennially to meet the re-issuing every two years of identification cards to its employees; and
- $40.8 million over the next three years for the capital cost of security equipment, such as access control and X-ray screening equipment.[11]

## Costs at regional airports

4.19 On 1 December 2003 the Government announced an extension of Australia's aviation security regulatory regime to cover all airports which provided regular passenger transport services. This resulted in a

[7] Mr Steven Fitzgerald, *Transcript,* 2 October 2003, p. 13.

[8] Ms Pamela Graham, *Transcript,* 21 October 2003, p. 13.

[9] Mr Stephen Goodwin, *Transcript*, 12 November 2003, p. 60.

[10] Mr Ian Robinson, *Transcript*, 12 November 2003, pp. 72–3.

[11] Qantas, *Submission No. 17*, pp. 113–14.

substantial number of regional airports being included in the security regime for the first time.

4.20 DoTaRS told the Committee that additional security was more than just installing an X-ray screening device:

> People focus very much on screening at an airport. There is no point in putting the screening equipment in the airport unless you redesign the airport to funnel people through the screening point, and there is no point in having the screening point unless you have the perimeter fence that prevents people from bypassing the screening point. Having put the perimeter fence in place, you then need to patrol it and light particular zones and so on. The introduction of a screening point costs, as a broad order of magnitude, around $1 million in up-front capital and would cost around $200,000 a year to operate.[12]

4.21 Examples of such changes were provided to the Committee:

- Coffs Harbour Airport would need up to $1 million to introduce checked-baggage screening;[13]
- Mackay Airport would require $1 million in capital costs, but this did not include alterations to baggage conveyor systems or changes to the terminal building;[14]
- Newman Airport would require $3 million to rebuild the terminal to enable passenger screening;[15]
- Nhulunbuy Airport in the Northern Territory would have to spend $2 million to comply with increased requirements;[16,17] and
- Tamworth would need from $750 000 to $1 million in capital costs to install screening equipment and modify the terminal.[18]

4.22 The submission from Qantas indicated that the costs of introducing passenger screening at the regional airports into which Qantas operated

[12] Mr Andrew Tongue, *Transcript,* 4 September 2003, p. 24.

[13] Mr Bevan Edwards, Australian Airports Association, *Transcript,* 21 October 2003, p. 21.

[14] Mackay Port Authority, *Submission No. 24,* p. 160.

[15] Mr Andrew Gaynor, WA Government, *Transcript,* 21 October 2003, p. 58.

[16] Mr David Piper, Australian Airports Association, *Transcript,* 21 October 2003, p. 24.

[17] The Committee notes that Nhulunbuy is not on the list of airports to be regulated provided by DoTaRS at *Submission No. 79,* p. 460.

[18] Mr Michael Dubois, *Transcript,* 2 October 2003, p. 36.

would cost 'in excess of $8.5 million in initial capital' and 'approximately $18.6 million in annual operating costs.'[19]

4.23 Operating costs include equipment maintenance costs which are higher in more remote areas. The Australian Airports Association told the Committee that 'the annual maintenance contracts for a particular piece of equipment could be 50 per cent greater than in a capital city.'[20]

4.24 As a general rule some if not all of these additional costs would be passed on to passengers through increased ticket prices. Examples of such impacts were provided to the Committee:

- on-going costs at Coffs Harbour would amount to $2 a passenger;[21]
- Mackay Airport would add $1.50 per passenger to cover additional operating costs;[22]
- Mildura Airport's additional costs would amount to $9 per passenger ticket;[23] and
- Mount Isa Airport would need to levy $14 per departing passenger to fund checked baggage screening and explosives trace detection devices.[24]

# Meeting the additional costs for security at airports

## Major airports

4.25 SACL argued that the Commonwealth Government needed to accept that it had responsibility for 'funding parts of aviation security in the national interest':

> We believe very strongly that aviation security is a national security issue. … The target of terrorism has always been the symbolic representations of countries and possibly even national

[19] Qantas, *Submission No. 17,* p. 117.

[20] Mr Bevan Edwards, *Transcript,* 21 October 2003, p. 21.

[21] Mr Bevan Edwards, *Transcript,* 21 October 2003, p. 21.

[22] Mackay Port Authority, *Submission No. 24,* p. 160.

[23] Mr George Vallence, Australian Airports Association, *Transcript,* 21 October 2003, p. 23.

[24] Mr Damien Vasta, Queensland Government, *Transcript,* 12 November 2003, p. 45.

> economies. The exception to this interpretation seems to come about only when it comes to the issue of funding.[25]

4.26 Qantas argued there were distinct roles for government and industry. Qantas told the Committee:

> I think that there are parts of this process that should be funded by government and there are parts that should be funded by the industry. The government has a role to fund border security issues, law enforcement issues, intelligence and security issues and those of a counter-terrorism nature. I think the airlines and airports have a role to provide protective security for their operations. At the end of the day the ultimate responsibility lies with the airlines. They are the people who are entrusted with the wellbeing of our passengers. … I think passenger screening is a process that should be funded by the industry not government.[26]

4.27 Qantas' submission provided more detail of the costs for which 'the Government should assume partial or full responsibility, because they primarily meet political or national security objectives.' These were:

- the ASO program (discussed below);
- the counter-terrorism first response function; and
- politically motivated violence checks.[27]

4.28 Qantas concluded that the lack of assistance from the Government in regards to aviation security adversely affected the competitiveness of Australian airlines and consequently associated industries such as tourism. Qantas was competing 'with over 50 foreign airlines in the Australian market, many of which [had] received assistance in one form or another from their governments in meeting security measures.'[28]

4.29 Virgin Blue in contrast suggested that there was a case for government assistance for the 'very large one-off cost for introducing global check bag screening infrastructure.'[29] When pressed by the Committee, however, Virgin Blue agreed with Qantas' concept of the division of responsibility, but still felt a case for government support could be made when one-off infrastructure costs were incurred.[30]

[25] Mr Steven Fitzgerald, *Transcript,* 2 October 2003, p. 13.

[26] Mr Geoffrey Askew, *Transcript,* 12 November 2003, p. 12.

[27] Qantas, *Submission No. 17,* pp. 114–15.

[28] Qantas, *Submission No. 17,* p. 116.

[29] Mr Philip Scanlon, *Transcript,* 12 November 2003, p. 29.

[30] Mr Philip Scanlon, *Transcript,* 12 November 2003, p. 33.

4.30 The Queensland Government commented that the demarcation proposed by Qantas, while broadly correct, was not totally clear-cut. Certain airports and airlines were capable of absorbing the costs of additional security, but:

> … some airlines in regional Queensland, for example, could be faced with security requirement costs that they may not be able to sustain. Similarly, airports in regional Queensland are potentially faced with those same concerns.[31]

## Regional airports

4.31 Many regional airports are owned and operated by local government. The NSW Government told the Committee that they also provided a 'vital economic and social link for rural and regional communities'.[32] The submission from the Australian Local Government Association went further:

> In remote and regional communities, basic services such as public transport and delivery of fresh food, medical supplies, mail, educational materials, and urgent supplies rely on the use of airport infrastructure. Airports gain further importance as entry gates to regions for business and industries that support and encourage ongoing regional and economic development.[33]

4.32 Tamworth City Council told the Committee that its fee structures were already marginal. Consequently, airport viability could be affected because airlines were likely to pass on fee increases to passengers who may well choose other forms of transport. Airlines would ultimately reconsider whether their services to regional airports were viable.[34]

4.33 The submissions from the Governments of South Australia and Tasmania also questioned the financial viability of their smaller airports if the airports had to meet the costs of upgrading security.[35]

4.34 All of the submissions from regional airports and the State Governments advocate the role of government, specifically the Commonwealth Government, in providing support for any increased security measures.

[31] Mr Damien Vasta, *Transcript,* 12 November 2003, p. 42.

[32] Mr John Schmidt, *Transcript,* 2 October 2003, p. 2.

[33] ALGA, *Submission No. 37,* p. 268.

[34] Mr Michael Dubois, *Transcript,* 2 October 2003, p. 36.

[35] State Government of South Australia, *Submission No. 56,* pp. 309–10; State Government of Tasmania, *Submission No. 32,* p. 240.

4.35 In contrast, the submission from Qantas stated that regional airport security was ‘a joint responsibility of State and Local Government, airport operators, airlines and other stakeholders.’ At the time of the submission, however, the aviation security regime had not been extended to include regional airports. Qantas stated it agreed with the Government’s view that security risks in regional aviation did not justify the additional expenditure which would be required for additional security.[36]

4.36 The role of State government has been acknowledged by representatives of the State Governments of Queensland and Western Australia.

4.37 The Queensland Government told the Committee that it subsidised air services to remote areas and assisted regional airports run by local government:

> The service itself is subsidised and the funds actually go to the airline in order to meet the shortfall that exists between the cost of operating the service and the revenue collected as fares. So the funds are used to make sure that the airline can operate the service in a profitable way and that the services continue. …
>
> The money that goes to local governments is under the grants program known as the Rural and Remote Airport Development Program where airports, through the local government as the owner, can apply to the state government for funding to upgrade their airports. It is usually used to improve the level of access that may or may not exist.[37]

4.38 The Western Australia Government told the Committee it also assisted regional air transport services and airports:

> The essential air services program provides finance to subsidise air services that would not be commercially viable, even for one particular airline. … The regional airports development scheme has provided $16 million of state government capital to regional airports and has leveraged in excess of $40 million from the local councils, from the Commonwealth government in some respects, and also from the private sector. [38]

4.39 The Western Australia Government commented that it provided grants to airports on a dollar for dollar basis. It cited the example of its grant of

[36] Qantas, *Submission No. 17,* p. 117.

[37] Mr Damien Vasta, *Transcript,* 12 November 2003, p. 46.

[38] Mr Andrew Gaynor, *Transcript,* 21 October 2003, p. 60.

$175 000 to Newman Airport to cover half the cost of designing the new terminal building.[39]

## Meeting the costs of the Air Security Officer program

4.40 As noted in Chapter 3, the costs to Qantas of the ASO program has amounted to $5.4 million for domestic flights. When ASOs have a presence on international flights Qantas estimated the cost of the program would increase to $20 million per annum in forgone ticket revenue.[40]

4.41 Qantas' submission argued that the Commonwealth should contribute to the cost of the ASO program because it met national security objectives. Qantas also argued that some of its international competitors were receiving assistance for security measures and Commonwealth assistance would restore some competitive balance. The submission also noted it was seeking relief from the Commonwealth.[41]

4.42 A supplementary submission from the AFP provided more information. AFP advised that the Commonwealth Government bore the costs of maintaining an operational program including ASO training and salaries. The airlines met the ticket costs for ASOs deployed on domestic flights. An interim agreement had been struck with Qantas for the funding of seats on international flights. Negotiations concerning permanent funding were continuing.[42]

## Committee comment

4.43 There appear to be two major arguments proffered for the Commonwealth to provide assistance to the aviation industry:

- that there are national security and economic benefits; and
- that there are regional economic and social benefits.

4.44 The Committee draws attention to the comments at the beginning of this chapter indicating the effect of a major aviation security incident on the Australian economy. The effect would be significant.

[39] Mr Andrew Gaynor, *Transcript,* 21 October 2003, p. 60.

[40] Qantas, *Submission No. 17,* pp. 114–15.

[41] Qantas, *Submission No. 17,* pp. 114, 115, 116.

[42] AFP, *Submission No. 90,* p. [p.1].

4.45 In considering the issues it should not be forgotten that ultimately the public pays through a combination of taxes, rates, and/or ticket prices. If there is no Commonwealth or State Government contribution the travelling public pays and, in the case of regional airports run by local government, ratepayers may subsidise the service.

4.46 If the Commonwealth contributes it is the wider community (ie including non-air travellers) that pays in recognition that the wider community benefits economically and socially from a broad aviation transport industry.

4.47 The Committee believes a distinction can be drawn when considering cost imposts between major airports and airlines, and regional airports and airlines. The large numbers of passengers passing through major airports and travelling on major airlines enable economies of scale to be achieved. The Committee also notes that major airports are becoming significant retail centres. These factors enable greater flexibility in absorbing capital and operating costs when enhanced security measures are introduced. The large number of passengers means that when costs are eventually reflected in the form of increased ticket prices, increases are relatively small.

4.48 Regional airports and regional airlines do not benefit from economies of scale and suffer economic penalty from being in remote areas. The Committee notes DoTaRS' comment early in the inquiry when it discussed whether the security system should be expanded to include regional airports:

> The challenge we face though is that in seeking to move to regional airports, we would effectively shut them down. That is simply because of the costs of security.[43]

4.49 The Committee accepts the argument that regional airports are important to vibrant and viable regional communities. The Committee also considers that viable regional communities benefit the nation.

4.50 The Committee believes it is important for State Governments to continue to recognise the value of regional aviation through the provision of assistance to regional airports and regional airlines. The Committee commends the Queensland and Western Australia Governments for providing such assistance. The evidence provided to the Committee did not indicate whether or not similar assistance was provided by other State or Territory Governments.

[43] Mr Andrew Tongue, *Transcript*, 4 September 2003, p. 18.

4.51 The Committee notes that the debate on how security enhancements at regional airports should be funded has been largely overtaken by recent Government announcements on 4 December 2003 and in the 2004–05 Budget.

4.52 The announcement in December 2003 extended security regulation to regional airports and indicated that a $14 million grants program, on a dollar for dollar basis, would be available to 'assist eligible smaller airports [to] implement appropriate security measures.' The enhanced security package was to be funded from surplus Ansett levy money. [44]

4.53 The announcement in the 2004–05 Budget expanded the money available to regional airports to $35 million and dropped the requirement for a matching contribution from the airport.[45]

4.54 The Committee observes that, from the cost information provided, the additional Commonwealth funds are unlikely to meet the total needs of all the regional airports coming under the expanded regulatory regime.

4.55 Turning to the ASO program, the Committee agrees with Qantas' argument that national security objectives warrant a contribution from the Commonwealth. An incident involving a major Australian airline, either Qantas or Virgin Blue, would have a direct impact on the attractiveness of Australia as an international tourist destination. There would be a consequent effect on a major export industry.

4.56 The Committee is pleased that the issue of the funding of the international component of the ASO program appears to be near to resolution.

[44] DoTaRS, *Submission No. 79*, p. 443.

[45] Budget Measures 2004–05, Budget Paper No. 2, p. 98.

5

# Interactions between aviation participants

## Introduction

5.1 An efficient and effective aviation industry requires close interactions between the various aviation industry participants. This chapter discusses some of those interactions, in particular:

- between the regulator, DoTaRS, and aviation industry stakeholders; and
- between the public and private sector participants in the aviation industry.

## Interactions between the regulator and the stakeholders

5.2 The Committee has received evidence on two aspects of the interaction between DoTaRS and aviation industry participants:

- consultations concerning the proposed new legislation and regulations; and
- the provision of intelligence, advice, and guidance.

## Consultations concerning the legislation

5.3 The aviation industry has criticised the extent of DoTaRS' consultation about the provisions of the Aviation Transport Security Bill 2003. BARA detailed its criticisms:

- papers outlining details of the new regulations were 'circulated at too short notice to facilitate meaningful discussion';
- rather than setting out the proposed regulations, papers were in the form of 'discussion papers or drafting instructions or draft regulations' prepared without the benefit of drafting instructions;
- industry was expected to 'assess individual regulations or groups of regulations in isolation';[1] and
- concepts were introduced which were 'foreign to the aviation industry' such as airport areas and zones, and the demerits points system.[2]

5.4 Comments from the major airport administrations and the two major airlines were consistent with this view.[3] Virgin Blue added that earlier consultation on security measures could be useful in identifying the costs to industry.[4]

5.5 Notwithstanding these criticisms, industry representatives told the Committee that consultation with DoTaRS had subsequently improved over the terms of the regulations.[5] Qantas suggested that DoTaRS may have initially been under a time constraint to meet its legislative tabling requirements, but had subsequently met its commitment to consult over the regulations. The witness acknowledged that it would not be possible to obtain consensus on all issues.[6]

5.6 APAM agreed that DoTaRS' consultation process was affected by time constraints:

> The department really makes quite a strong effort to consult as widely as they can. I just suspect that at times they are under time

[1] BARA, *Submission No. 3,* p. 14.

[2] Mr Warren Bennett, *Transcript,* 2 October 2003, p. 55.

[3] Ms Pamela Graham, APAM, *Transcript,* 21 October 2003, p. 15; Mr Stephen Goodwin, BAC, *Transcript,* 12 November 2003, p. 48; Mr Steven Fitzgerald, SACL, *Transcript,* 2 October 2003, p. 17; Qantas Airways, *Submission No. 17,* p. 111; Virgin Blue Airlines, *Submission No. 14,* p. 86.

[4] Mr John O'Callaghan, *Transcript,* 12 November 2003, p. 33.

[5] Mr Stephen Goodwin, BAC, *Transcript,* 12 November 2003, pp. 48–9; Mr Ian Robinson, Cairns Port Authority, *Transcript,* 12 November 2003, p. 71; Mr Steven Fitzgerald, SACL, *Transcript,* 2 October 2003, p. 17; Mr John O'Callaghan, Virgin Blue Airlines, *Transcript,* 12 November 2003, p. 34.

[6] Mr Geoffrey Askew, *Transcript,* 12 November 2003, pp. 22, 23.

> constraints, and perhaps some resource constraints as well, that make it not as effective as it could be. If I was to compare it to some other agencies, I would say their consultation processes are fairly good.[7]

5.7 DoTaRS responded robustly to industry criticisms concerning the consultation process:

> I think industry, frankly, is a little bit precious about all of this. We are a regulator. We are not people who are meant to make everybody happy. We are meant to basically reflect government policy in legislation and then go and implement it. In terms of consultation on the legislation, I would be happy to come back to you with a detailed list of where we consulted, how we consulted and who we consulted. My feeling is that there has been extensive consultation. The real detail that industry needs is in the regulations, and there we have consulted ad nauseam—I would say excessively, because it slowed it down. I challenge the notion that we have not consulted as extensively as possible.[8]

5.8 The Committee suggested that early consultation would have resulted in better legislation and regulations. DoTaRS defended its position:

> Better is in the eye of the beholder. As a regulator, what I would like are some nice, clear, tough regulations that I could get out and implement. I am sure what the industry would like are some nice, floppy regulations that are not going to cost them too much money and that they can drive holes through. What I have found … in regulation making is that the more you consult the more you tend to get driven towards the lowest common denominator. I am not sure in the current climate that that is what the community wants from us and, frankly, the community is not present at the consultations.[9]

## Committee comment

5.9 The Committee does not agree with DoTaRS' view of the value of consultation. Adequate and extensive consultation will assist in identifying areas of contention and areas where education is needed. Moreover, consultation may ease the passage of legislation through the Parliament. Consultation does not necessarily mean compromise—

[7] Ms Pamela Graham, APAM, *Transcript,* 21 October 2003, p. 15.

[8] Mr Andrew Tongue, *Transcript,* 24 November 2003, p. 21.

[9] Mr Andrew Tongue, *Transcript,* 24 November 2003, pp. 21–2.

whether or not this happens depends on the determination of those proposing the legislation and the strength of their arguments for reform.

## Provision of intelligence, advice, and guidance

### Intelligence and threat alerts

5.10 DoTaRS described its role as a 'preventative security agency' rather than as a 'counter-terrorism first response' (CTFR) agency. CTFR was the role of the Attorney-General's Department and its agencies. DoTaRS explained the sequence of events when a security issue arose:

> We would be advised by ASIO that they had something important. That can be communicated to us through the appropriate secure communications systems. Typically we make a joint assessment with them of the implications of the particular piece of intelligence. Our next immediate step is to talk to airports and airlines about the nature of the intelligence.[10]

5.11 DoTaRS added that a substantial amount of intelligence information was being obtained around the world through the debriefing of captured terrorists. Assessing the value of that intelligence was a role for ASIO and not the department.[11]

5.12 At a later hearing, DoTaRS told the Committee that much effort was being applied to terrorist related intelligence. The department was working closely with other Commonwealth agencies such as the AFP, APS, Customs with the aim of enhancing operational or daily intelligence.[12] DoTaRS also described the role of the newly created National Threat Assessment Centre[13]:

> [It] will basically pool the resources of the security agencies from a number of different departments. We will also have some people in there. It will give the country the capacity to produce threat assessments 24 hours a day, seven days a week, 365 days a year. The reason we are putting people in there is that the Commonwealth regulatory system around aviation and future maritime will be built on the threat assessments …[14]

[10] Mr Andrew Tongue, *Transcript*, 4 September 2003, p. 23.

[11] Mr Andrew Tongue, *Transcript*, 4 September 2003, p. 24.

[12] Mr Andrew Tongue, *Transcript*, 24 November 2003, p. 30.

[13] The National Threat Assessment Centre was formally opened by the Prime Minister on 5 May 2004.

[14] Mr Andrew Tongue, *Transcript*, 24 November 2003, p. 33.

5.13 The major industry players appeared satisfied with the intelligence they were receiving from DoTaRS and ASIO. For example, Qantas told the Committee it had a very good relationship with ASIO and that there was a recognition of the 'importance of intelligence and the importance of the timely dissemination of that intelligence.'[15] Virgin Blue indicated it had a 'fairly good relationship' with DoTaRS and ASIO regarding the flow of information.[16] APAM was complimentary concerning recent intelligence coordination arrangements:

> What is happening now … is that the department and the Attorney-General's Department are bringing together almost what you would call a road show on intelligence. So we feel that we are being briefed quite regularly on what is happening—probably better than we have been in the past.[17]

5.14 On the other hand, evidence from two regional airports indicated that the flow of intelligence information could be improved.

5.15 Coffs Harbour Regional Airport told the Committee that it did not get a 'great deal of intelligence on possible threats and the like.' The airport had a close working relationship with the NSW Police, however, and the witness acknowledged that much intelligence was provided on a 'need to know' basis. He added that the police responded very quickly to emergency situations.[18]

5.16 Cairns Port Authority told the Committee that it used to 'receive a regular flow of information' from ASIO via DoTaRS, but this had stopped at the end of 2001. Possible reasons were the remoteness of Cairns and the fact that the airport was no longer a member of any government program that would have provided 'a conduit for any sort of classified material or intelligence relating to aviation security.' A recent briefing by ASIO that had been arranged by DoTaRS in response to this concern 'was of high quality' and met the requirement of the airport's security committee.[19]

### Committee comment

5.17 Given the current threat environment, the Committee believes there is a strong flow of intelligence to the aviation industry. The Committee considers that recent developments, specifically the creation of the National Threat Assessment Centre will assist the flow of intelligence.

[15] Mr Geoffrey Askew, *Transcript*, 12 November 2003, p. 18.

[16] Mr Philip Scanlon, *Transcript*, 12 November 2003, p. 35.

[17] Ms Pamela Graham, *Transcript*, 21 October 2003, p. 4.

[18] Mr Bevan Edwards, *Transcript*, 2 October 2003, p. 33.

[19] Mr Ian Robinson, *Transcript*, 12 November 2003, pp. 63–4, 69; Mr Philip Warwick, *Transcript*, 12 November 2003, p. 69.

5.18 The expansion of the number of airports to be regulated will, however, place demands on the flow of relevant intelligence especially to regional airports. DoTaRS will need to address these demands if smaller airports are to receive up to date intelligence information.

## General advice to aviation industry participants

### High level consultation

5.19 In May 2003, DoTaRS established a the High Level Group on Aviation Security (HLGAS). The aim was to provide a forum for the exchange of ideas on aviation security between the department, the aviation industry and key government agencies. More specifically:

> The group aims to facilitate the development of a coherent position in the management of major aviation security issues, through a strategic approach involving Government and industry representatives.[20]

5.20 HLGAS comprises representatives from five Commonwealth agencies, four aviation industry companies and three aviation peak bodies. The group is chaired by DoTaRS and meets quarterly. The objectives of HLGAS are:

> To protect the sector of Australia's social and economic infrastructure that relates to aviation by delivering:
>
> - advice to Government on industry's views on how to deter, detect, and prevent attempted acts of unlawful interference to civil aviation;
> - industry's view of the future issues in aviation security;
> - advice to Government on the most efficient method of responses to security incidents.[21]

5.21 The major aviation industry participants have welcomed the creation of HLGAS.[22] BARA commented:

> [HLGAS] is looking at what the threats might be in the future, based upon intelligence advice that is given to the group by the Commonwealth government intelligence agencies. We are moving beyond simply looking at day-to-day security functions at airports. We are looking at what, in the future, might be the source of different threats to aviation.[23]

[20] DoTaRS, *Submission No. 89,* p. 542.

[21] DoTaRS, *Exhibit No. 11, High Level Group on Aviation Security, Terms of Reference & Membership.*

[22] SACL, *Submission No. 15,* p. 89; Virgin Blue, *Transcript,* 12 November 2003, p. 32.

[23] BARA, *Transcript,* 2 October 2003, pp. 60–1.

5.22 DoTaRS also advised the Committee that it chaired an Industry Consultative Meeting (ICM) group which comprised representatives of major airlines, airports, the AFP, and other government agencies. The ICM met quarterly and had a number of sub-groups such as the ASIC,[24] Screening Improvement, and Checked Bag Screening working groups.[25]

### Advice on the outcome of audits and assessments

5.23 Qantas raised concerns that, at the operational level, it was not provided with the results of systems testing and security infrastructure reviews of Australian airports into which the airline operated. It was concerned it might be 'at risk of operating into airports with possible security deficiencies which [were] known to government and the relevant airport operator, yet of which it [was] itself unaware.'[26]

5.24 At a public hearing Qantas elaborated:

> I think it is important that, when any government undertakes an audit or an inspection of a process that has an impact on Qantas or other carriers, those carriers are then advised of the outcome of that audit or inspection. If we are not so advised then it is impossible for us to work with the government agency, the airport operator or the terminal operator—with our colleagues, other carriers—to improve that process.

5.25 DoTaRS responded to this issue, noting that 'airport audit findings are generally discussed at the relevant Airport Security Committee (ASC) meetings.' DoTaRS formally notified industry of the outcome of audits and it was standard practice for airports to table this advice at ASC meetings. Because airlines attended ASC meetings, DoTaRS thus assumed they were made aware of audit findings. DoTaRS added that it was working with the aviation industry:

> … to develop an industry wide cooperative information sharing approach to some of the other compliance monitoring activities undertaken by both the Department and industry.[27]

### Advice on equipment

5.26 DoTaRS has been criticised for its level of contact with equipment suppliers, and the quality of advice to industry participants on the equipment to be used.

[24] Aviation security identification card.

[25] DoTaRS, *Submission No. 89*, p. 542.

[26] Qantas Airways, *Submission No. 17,* p. 108.

[27] DoTaRS, *Submission No. 87,* p. 538.

5.27 L3 Communications told the Committee that it would like to assist DoTaRS' understanding of available technologies. There had been little opportunity, however, for it to make representations to the regulator. The company believed it was possible for DoTaRS to specify requirements without specifying the actual equipment to be supplied.[28]

5.28 In another example, BAC told the Committee it had asked DoTaRS whether it was suitable to install a particular type of baggage scanning equipment. The reply had been ambiguous—DoTaRS had advised that the equipment was acceptable because it was equivalent to that used in America and other Western countries. BAC would have preferred a more definitive response such as a statement that the equipment met Australia's standard. BAC's concern was that it was not receiving information on the Australian Government's position on the equipment platform to be used. A possible consequence was that the types of equipment to be installed could be determined at the whim of another country.[29]

5.29 DoTaRS response was that:

> … equipment operated in Australia must be approved for use by other major world aviation security regulatory bodies such as those of the United States, United Kingdom, European Civil Aviation Commission or Canada. There has been no variation to this position and all equipment suppliers are aware of it.[30]

5.30 DoTaRS later advised the Committee that its ICM group was establishing a working group to look at technological advances. Experts in certain areas might be called upon to assist the working group as the need arose.[31]

### Committee comment

5.31 The Committee welcomes the creation of HLGAS and the ICM group and believes these avenue of communication will at least in part address Qantas' concerns. The Committee also accepts DoTaRS' comments that results of its audits are routinely tabled at ASC meetings. The recent expansion of the aviation regulatory system will mean all airports servicing passenger flights will now need DoTaRS-approved airport security programs. This should raise the standard of aviation security in Australia. This is dependent, however, on the regulator's ability to conduct compliance audits of all airports falling within the system.

[28] Mr Mark Knox, *Transcript*, 12 November 2003, pp. 6, 7.

[29] Mr Stephen Goodwin, Mr Edward McPheat, *Transcript*, 12 November 2003, pp. 54, 55.

[30] DoTaRS, *Submission No. 79*, p. 431.

[31] DoTaRS, *Submission No. 89*, p. 542.

5.32 Regarding advice to equipment suppliers, the Committee notes that Australia is a small player in an international industry. This means unfortunately that if America or European countries require baggage screening to a particular standard, Australia has no alternative but to comply. To mandate an Australia-specific standard risks the denial of entry to major overseas countries if Australia's standard is deemed unacceptable.

5.33 The Committee accepts DoTaRS assertion that it has made clear how it assesses the adequacy of equipment for Australian airports. The Committee questions whether it is essential for equipment suppliers to make representations to DoTaRS when the Commonwealth is not the purchaser of the equipment they offer.

## Interactions between aviation industry participants

5.34 The Committee has received evidence on two aspects of the interaction between aviation participants:

- the numbers of State Police at major airports in relation to the numbers of Australian Protective Service (APS) officers; and
- the role of security committees at airports.

### Commonwealth and State police forces

5.35 The Australian Federal Police (AFP) told the Committee that the APS provided CTFR at eleven airports in Australia.[32] At other airports the responsibility for CTFR was the State police.[33] Where both APS and State police were present at an airport the roles of both agencies was strictly defined:

> The APS's role as a counter-terrorism first responder is not an investigative role. So they will go into a situation, assess that situation, cordon off, contain and then hand over command to the relevant state or territory police service. Resourcing is not to go to a prosecution brief so the distinction is quite clear. We work very closely with state and territory police in achieving a good, cooperative relationship with those services.[34]

[32] Adelaide, Alice Springs, Brisbane, Cairns, Canberra, Coolangatta, Darwin, Hobart, Melbourne, Perth, and Sydney.

[33] Ms Audrey Fagan, *Transcript*, 4 September 2003, p. 39.

[34] Ms Audrey Fagan, *Transcript*, 4 September 2003, p. 43.

5.36 DoTaRS raised a concern about a decline in the numbers of State police at airports when APS presence increased:

> My bigger worry … is the relative absence of state police from our airports. As the Commonwealth has put resources in, particularly the counter-terrorism first response APS presence, it appears to us that we see fewer and fewer state police. An airport is no different to a shopping centre in terms of the community policing role …[35]

5.37 Support for this view was provided by SACL:

> … there used to be a permanently manned presence on airport with a police station on airport. That station, while it still exists as a facility, is not permanently manned. Our view is that, as a very large piece of community infrastructure where crime at all levels is an issue, it warrants a permanent community policing presence, which is not currently the role of the Commonwealth agencies that operate on airport.[36]

5.38 Qantas also commented that local police presence at major airports was as big a concern for it as police presence at regional airports. State police had 'a role to provide a presence throughout [the] community.' This role was to educate the airport community about preventative security as well as to provide deterrence through patrols.[37]

5.39 On the other hand, the AFP witness, when specifically asked by the Committee whether there had been a decline in State police numbers as APS presence increased, responded, 'No, not in my experience.'[38]

5.40 The Committee sought further information from State police forces in NSW, Victoria and Queensland on the police presence at their capital city airports and the nature and level of crime at those airports.

5.41 The NSW Police advised that general law enforcement for Sydney Airport was provided by the Botany Bay Local Area Command. This included regular patrols of the airport and 'specialist law enforcement.' Since September 2001 police patrols of critical infrastructure such as the airport had increased and the airport had 'seen an increase in patrols and targeted operations.' Over the past three years the general level of crime at the airport had been low and stable except for 'other theft' which had declined.[39]

[35] Mr Andrew Tongue, *Transcript,* 24 November 2003, p. 23.

[36] Mr Steven Fitzgerald, *Transcript*, 2 October 2003, p. 24.

[37] Mr Geoffrey Askew, *Transcript*, 12 November 2003, pp. 23, 24.

[38] Ms Audrey Fagan, *Transcript,* 4 September 2003, p. 43.

[39] NSW State Cabinet Office, *Submission No. 80,* p. 463.

5.42 The Victoria State Government advised that the Victoria Police presence at Melbourne Airport consisted of two officers who staffed the Airport Police Station and conducted foot patrols 'between 9 am and 5 pm, seven days a week.' This level of police presence had been established in 1999 and had not changed since then. As well, there was a Police station close to the airport which enabled response time of 'less than ten minutes for serious incidents.' Melbourne Airport experienced the 'types of crime similar to a small city but at a significantly lower level.'[40]

5.43 The Queensland Government advised that police presence at Brisbane Airport was provided by the nearby Hendra Police Station which had a response time of four minutes for emergency or urgent incidents. Daily regular patrols were conducted, dependent on operational requirements. There had been no change to this level of policing over the previous three years. Over this time there had been 390 reported offences at Brisbane Airport sites mainly comprising of stealing from specific buildings and lost property. (The submission did not comment on how this compared with crime in other areas.)[41]

## Committee comment

5.44 The Committee considers the evidence before it does not sustain the argument that as Commonwealth police presence increases, State police presence declines. That is, that there is a cause and effect relationship. Critical to the Committee's view was the evidence from the AFP witness that in her experience this was not occurring.

5.45 Nevertheless, evidence provided by the States indicates that the incidence of crime at major airports is significantly less than in comparable areas. This may be a collateral benefit arising from high numbers of security personnel and APS officers at airports. In such circumstances, the Committee would expect a reduction in the number of State police patrols to allow resources to be directed to areas of greater need.

5.46 There will be a limit to any reduction of State police presence, however, because State police must be in a position to respond to serious incidents. In addition, if State police routinely relied upon Commonwealth officers to step in when non-terrorist crime occurred, successful prosecutions could be jeopardised.

5.47 The Committee concludes that the level of State police at major airports where there is an APS presence is a matter for the State police in accordance with their arrangements with the APS. If airports see a need

[40] Victoria Department of Premier and Cabinet, *Submission No. 86,* pp. 532–3.

[41] Queensland Government, *Submission No. 85,* pp. 530–1.

for increased security they should make representations to the APS or State police, or employ additional security guards.

## Security committees at airports

### Airport security committees

5.48 Under the previous legislation—the *Air Navigation Act 1920*—operators of security categorised airports were required to have an ASC. Membership was nominated by the operator and approved by DoTaRS.[42] Frequency of ASC meetings was prescribed in the regulations and they were to be presided over by the airport operator or its nominee.[43]

5.49 The legislation specified that the function of the ASC was to make recommendations to the airport operator concerning the preparation and implementation of the airport security program.[44]

5.50 During the inquiry, comments from witnesses indicated that the ASCs to which they belonged were active committees. For example, APAM told the Committee that its ASC met every two months and had between 15 and 25 attendees.[45] Cairns Airport noted that it had a 'very effective security committee' which had received a briefing by ASIO.[46] Coffs Harbour Airport outlined the role of its ASC in emergency situations.[47]

5.51 Nevertheless, the submission from APAM recommended that the role of ASCs be strengthened to enhance consultation on aviation security as well as on airport business.[48]

5.52 Qantas considered that ASCs were under-utilised as a tool for achieving aviation security outcomes and they should be 'afforded a greater level of responsibility and their profile elevated'. Qantas added that the reconstituted ASCs should:

- provide feedback, via DoTaRS to the Industry Consultative Group and where necessary to the recently established High Level Group on Aviation Security on specific factors affecting the delivery of outcomes at individual airports;

[42] *Air Navigation Act 1920*, Section 22ZB, pp. 64–5.

[43] *Air Navigation Regulations 1947*, Subdivision 3, 63–7, pp. 58–66.

[44] *Air Navigation Act 1920*, p. 65.

[45] Ms Pamela Graham, *Transcript*, 21 October 2003, p. 12.

[46] Mr Ian Robinson, General Manager Airport, Cairns Port Authority, *Transcript*, 12 November 2003, p. 69.

[47] Mr Bevan Edwards, Airport Manager, Coffs Harbour Regional Airport, *Transcript*, 21 October 2003, pp. 33, 35.

[48] APAM, *Submission No. 19*, p. 131.

- measure the effectiveness of aviation security policies and procedures at individual airports through a program that monitors and reports on compliance; and
- establish and monitor an airport specific aviation security and facilitation protocol between border agencies and the industry.[49]

## Australian Government security agency committees

5.53 A supplementary submission from APAM has drawn the Committee's attention to the establishment of an Australian Government security agency committee at each airport. [50]

5.54 DoTaRS provided further information noting that the aim was to enhance coordination arrangements between Australian government agencies with a transport security interest. This would be achieved through the creation of 'a Canberra-based central policy committee and an Australian Government security agency committee at each major airport.' The new security committee would not replace the ASC:

> … but will ensure better coordination of the work of Australian Government agencies at airports, including intelligence dissemination and cooperation with industry on security matters.[51]

5.55 APAM was concerned, however, that while the objective of improving the coordination of government agencies at airports was valid:

> … it is important that the overall integrity and accountability of the Airport Operator chaired Security Committee is maintained. It would be inappropriate for unilateral security policy decisions to be made by another Committee without the appropriate linkages to the principal Airport Security Committee.[52]

5.56 APAM also told the Committee that the tendency for the APS to act autonomously could create difficulties concerning communication and coordination for the airport operator.[53] APAM's submission commented:

> It is essential that airport operators have effective control over all operational aspects of their security contractors, including the APS, if they are to efficiently manage and coordinate airport security programs. This is particularly important when the airport operator has overall accountability for airport security.[54]

[49] Qantas, *Submission No. 17*, p. 108.

[50] APAM, *Submission No. 75*, p. 414.

[51] DoTaRS, *Submission No. 79*, p. 439.

[52] APAM, *Submission No. 75*, p. 414.

[53] Ms Pamela Graham, *Transcript*, 21 October 2003, p. 13.

[54] APAM, *Submission No. 19*, p. 133.

## Committee comment

5.57 A fully functioning and active ASC is an important focus point for private and public sector stakeholders at airports. It will provide for ongoing consultation and the resolution of differences in individual aviation participant security programs, before the need for arbitration by DoTaRS.

5.58 DoTaRS has advised the Committee that it ‘has an obligation to reconcile conflicts before approving any transport security program’ and will arbitrate where disputes arise.[55] An effective ASC, however, should resolve any unforseen conflicts before the need to seek assistance from DoTaRS.

5.59 The Committee believes that the specific activities for an ASC are a matter for its members to decide. The Committee does not wish to preclude the expanded role of ASCs envisaged by Qantas, but it is essential that DoTaRS as the regulator monitors the effectiveness of aviation policies and procedures and audits compliance. Subsequent performance audits of DoTaRS by the ANAO completes the chain of accountability through reports to the Parliament and the public. If DoTaRS were to be removed from this role, as implied by Qantas’ suggestion, a link in this accountability chain would be broken.

5.60 The Committee sympathises with APAM’s concerns about the airport operator retaining overall responsibility for airport security when government security agencies may be required to act autonomously for urgent operational reasons. The creation of Australian Government agency security committees at airports may assist coordination provided clear and efficient lines of communication are established. On the other hand, the proliferation of committees often increases the risk of communication delays and breakdowns.

5.61 To reduce the potential for such problems, the Committee considers it essential to establish a memorandum of understanding between the ASC and the corresponding Australian Government agency security committee, including their members.

5.62 The memorandum of understanding should address issues such as:

- the respective responsibilities of the two committees and their individual members;
- ways to ensure timely consultation on security matters; and
- ways to ensure timely two-way dissemination of intelligence information.

[55] DoTaRS, *Submission No. 79,* p. 440.

### Recommendation 1

5.63 **When an Australian Government security agency committee is established at a particular airport, the Department of Transport and Regional Services should be responsible for establishing a memorandum of understanding between the Government security agency committee and the corresponding airport security committee.**

6

# Security procedures at airports

## Introduction

6.1 The security procedures at regulated airports in Australia are underpinned by legislation and associated regulations. Aviation participants, however, are able to introduce more stringent procedures than those stipulated by the Government.

6.2 Until the passage of the *Aviation Transport Security Act 2004* in March 2004, aviation security was governed by Parts 3 and 3A of the *Air Navigation Act 1920* and its regulations.[1]

6.3 The new legislation repealed Parts 3 and 3A of the *Air Navigation Act 1920* and replaced them with specific aviation security legislation. The *Aviation Transport Security Act 2004* focuses on:

- transport security programs (Part 2);
- airport areas and zones (Part 3);
- other security measures (Part 4);

[1] Part 3 covered: the screening of passengers and baggage (Division 1); the reporting of unlawful interference with aviation (Division 2); aviation security programs (Division 3); airport security programs (Division 4); the security measures to be applied to the various categories of airports (Division 5) ; and miscellaneous provisions dealing with the removal of people and the surrendering of weapons to an aircraft operator (Division 6). Part 3A, added in December 2002, covered information gathering for aviation security purposes.

- powers of officials (Part 5);
- reporting aviation security incidents (Part 6);
- information gathering (Part 7); and
- enforcement (Part 8).

6.4 Although the new legislation has been enacted, its associated regulations have yet to be promulgated. The Committee has, however, received an April 2004 draft of the new regulations.

## Legislated requirements

### Airport security committees

6.5 As noted in Chapter 5, the *Air Navigation Act 1920* and its regulations stipulated the existence, function, membership and meeting frequency of ASCs. In submissions to the Committee both APAM and Qantas have called for the role of ASCs to be strengthened and their profile increased.[2]

6.6 Paradoxically, the provisions of the *Aviation Transport Security Act 2004* and its draft regulations no longer contain references to ASCs. The Committee has considered whether this represents a weakening of the role of ASCs.

6.7 While the new legislation makes no specific mention of ASCs, it requires aviation participants to have approved security programs. Part 2, Division 4, Section 16 (2), states that the security program should include:

> - how the participant will manage and co-ordinate aviation security activities within the participant's operation;
> - how the participant will co-ordinate the management of aviation security with other parties (including Commonwealth agencies) who have responsibilities for, or are connected with, aviation; …
> - the other industry participants who are covered by, or operating under, the program;
> - the consultation that was undertaken, in preparing the program, by the participant with the other aviation industry participants who are covered by, or operating under, the program.[3]

[2] APAM, *Submission No. 19*, p. 131; Qantas, *Submission No. 17*, p. 108.

[3] Subclauses (a), (b), (f), and (g), p. 19.

6.8 DoTaRS defended the lack of specific reference to ASCs in the legislation. It advised the Committee that it was currently 'preparing guidance material to assist airport operators to identify relevant risks and develop security programs.'[4] These guidelines would detail the:

> … requirement for airports to have an ASC, as well as their role and composition … unless these guidelines are adhered to, the Department will not approve an industry participant's program.
>
> … The fact that ASC requirements are no longer housed under principal legislation means that they can be more easily altered as the aviation environment changes. In this way, the Aviation Transport Security Bill 2003 provides greater scope for an increased ASC role than does the existing legislation.[5]

6.9 The Committee asked both APAM and Qantas whether they considered the non-inclusion of ASCs in the new legislation to represent a downgrading of the importance of ASCs.

6.10 APAM responded that it did not consider this to be the case. It added:

> The new legislation is intended to focus on risk based security outcomes rather than taking a prescriptive approach. … Melbourne Airport will certainly be including the requirement for an Airport Security committee within its Airport Security Program.[6]

6.11 Qantas on the other hand reiterated its view that despite DoTaRS' explanation, 'the formation, performance and objective of the [ASC] is best outlined in regulation rather than security programs.'[7]

## Committee comment

6.12 The Committee accepts DoTaRS' argument that there needs to be flexibility to address a potentially rapidly changing aviation security environment. The removal of the requirement for ASCs from the *Aviation Transport Security Act 2004* is therefore supported. The issue is whether sufficient flexibility can be achieved by defining the requirements for ASCs in the Regulations or DoTaRS' transport security program guidelines.

6.13 Notwithstanding DoTaRS' statement that an airport operator's aviation security program will not be approved unless it includes details of an

[4] DoTaRS, *Submission No. 79*, p. 431.

[5] DoTaRS, *Submission No. 79*, pp. 439.

[6] APAM, *Submission No. 75*, p. 414.

[7] Qantas, *Submission No. 77*, pp. 424–5.

ASC, guidelines are just that, **guidelines**—which depend on interpretation and rigor of application. On the other hand, regulations specify **requirements**.

6.14 In the Committee's view, if there is a need for rapid change, new regulations can be promulgated almost as quickly as new departmental guidelines. The advantage of including non-negotiable aspects of security programs in the regulations is that these requirements will be transparent and open to scrutiny by the Parliament and the people. Aviation security is currently a national issue of public interest so it is important that all Australians can be assured that security programs are of a high standard.

### Recommendation 2

6.15 **The requirement for airport security committees and other essential requirements for aviation security programs should be defined in the Aviation Transport Security Regulations 2004**

## Airport areas and security zones

### Landside and airside areas and their security zones

6.16 The *Aviation Transport Security Act 2004* extends the areas of airports which come under security controls. The previous legislation focused on protecting aircraft, that is the airport apron; the new legislation extends this to cover the movement of people and important infrastructure.[8]

6.17 The new legislation no longer refers to 'sterile areas' within airports, but instead refers to landside and airside areas. Within these areas are security zones which:

> … will have tighter or more specialised access control arrangements … to reflect the particular risk to aviation security presented by that part of the airport. … This system is designed to promote flexibility within and across airports to focus on getting the right security measures operating in the right areas.[9]

6.18 The landside area would in general comprise the bulk of the airport terminal building and areas outside which are freely accessible to the public. Security zones would be declared within the landside area to ensure the security of:

[8] Dr Andy Turner, *Transcript*, 24 November 2003, p. 27.

[9] *Aviation Transport Security Bill 2003, Explanatory Memorandum*, pp. 34, 35.

- control towers;
- fuel storage areas;
- general aviation areas;
- cargo and baggage handling facilities; navigational aids; and
- critical facilities and critical structures.[10]

6.19 The Explanatory Memorandum provided the following explanation:

> While landside areas have traditionally been considered freely accessible to the general public, provision has been made … to designate a landside security zone should the need arise. For example, in the future, it may be necessary to act quickly to restrict entry into the terminal building to include passengers and aviation industry participants only. The establishment of a landside security zone would allow this to occur without having to amend the Act.[11]

6.20 The new system has been criticised by BARA on two grounds:

- as departing from the internationally accepted definitions;[12] and
- because the existing sterile areas in the airport terminal would be reclassified as 'airside' thereby ignoring 'the actual workings of domestic terminals.'[13]

6.21 BARA suggested that several problems could arise from reclassifying sterile areas as airside. These included:

- it could be an offence for 'meeters and greeters' to enter the area;
- aviation security identification cards (ASICs) would have to be issued to all employees such as retail concession staff working in the area; and
- the inconsistency of meeters and greeters not having to have ASICs—BARA assumed they would continue to have access to the area.[14]

## Committee comment

6.22 The Committee does not share BARA's concerns because:

[10] *Aviation Transport Security Bill 2003, Part 3, Division 2, Section 34.*

[11] *Aviation Transport Security Bill 2003, Explanatory Memorandum*, p. 38.

[12] Mr Warren Bennett, *Transcript*, 2 October 2003, p. 56.

[13] BARA, *Submission No. 3*, p. 17.

[14] BARA, *Submission No. 3*, p. 17.

- the issue appeared not to be of major concern to the airport operators participating in the inquiry;
- the new legislation allows different security measures to be applied to different security zones;[15]
- April 2004 Draft Regulation 3.36 (2) allows 'persons welcoming or farewelling intending passengers' to be in cleared zones without an ASIC provided they are 'generally supervised';[16] and
- the *Aviation Transport Security Act 2004* requires DoTaRS to 'have regard to the purpose of the area or zone' and take into account the views of the airport operator and existing physical and operational features of the airport.[17]

6.23 In addition, the Committee does not consider it inappropriate for DoTaRS to strive to become a world leader in redefining and expanding airport security terminology—provided that is, the definitions which are used are clear and understood by aviation participants.

## Access to security zones

6.24 The April 2004 Draft Regulations specify three types of security passes which permit access to security zones:

- ASICs—issued to people 'who requires access, for the purposes of his or her employment, to a secure area';
- temporary ASICs—issued to ASIC holders when the ASIC is lost or stolen; and
- visitor identification cards—issued to people needing to visit a secure area who will be 'supervised by the holder of a valid ASIC while in the area.'[18]

### Aviation security identification cards

6.25 ASICs are issued by airport operators and other industry participants authorised by DoTaRS. Proposed regulation 3.04 requires ASIC issuing bodies to have an approved ASIC program in place.

[15] April 2004 Draft Regulations 3.48–3.51, provide separate additional security measures for apron, airside cargo areas, airside fuel areas, and airside control tower zones.

[16] This provision was absent from the September 2003 version of the Draft Regulations—BARA made its submission in July 2003.

[17] Part 3, Division 2, Section 34, p. 30.

[18] April 2004 Draft Regulations 3.15, 3.18, 3.31, pp. 21, 24, 32.

6.26 DoTaRS told the Committee that a scheme had been introduced on 1 November 2003 to reissue ASICs. Checks now included one for politically motivated violence as well as the police record check. ASICs had also been redesigned to make them harder to forge and were colour-coded to indicate areas which could be accessed.[19] DoTaRS emphasised that possession of a particular coloured ASIC did not provide automatic access to a security area:

> You have to have the identification card and a legitimate reason to be there. For example, you may have an ASIC which has the right colour and, if challenged, you could say that you have a legitimate reason for being there today. You may have the same ASIC tomorrow but you may not have a legitimate reason for being there. The colour of the card in and of itself is not conclusive proof that you can be there. [20]

6.27 DoTaRS also drew attention to the extension of the ASIC system to cover 'employees at all airports servicing passengers and freight aircraft by 1 July 2004.'[21]

### *Return of aviation security identification cards*

6.28 The previous and proposed regulations require lost or stolen ASICs to be reported, and expired ASICs to be returned. The proposed regulations require the ASIC to be returned 'as soon as practicable, but within 7 days.' The penalties for the non-return of an expired ASIC, previously 5 penalty units, is to be increased to 10 penalty units.[22] (This is equivalent to $1 100 for an individual.[23])

6.29 Despite the regulations, the Committee has discovered that a significant percentage of expired ASICs have not been returned. DoTaRS told the Committee that an audit of Melbourne Airport, prompted by evidence to the Committee, revealed that 'around 15 or 16 per cent' of expired cards were not returned. DoTaRS commented that this was 'much higher than we would like it, to put it mildly.' (For active ASICs the figure was less than two per cent—a level which did not cause DoTaRS concern.)[24]

6.30 The Committee asked DoTaRS whether there should be incentives, such as a refundable bond, to promote the return of expired ASICs. DoTaRS responded:

[19] Dr Andy Turner, *Transcript*, 24 November 2003, pp. 26–7, 28.

[20] Dr Andy Turner, *Transcript*, 24 November 2003, p. 29.

[21] DoTaRS, *Submission No. 79*, p. 456.

[22] April 2004 Draft Regulations 3.41, p. 37.

[23] DoTaRS, *Submission No. 79*, p. 436.

[24] Dr Andy Turner, *Transcript*, 24 November 2003, p. 28.

> The proposed regulations are outcomes-based and focus on making the ASIC issuing body responsible for the cards that they issue. As the regulator, DOTARS must approve the programs of the ASIC issuing body, and as such it is required to be satisfied that they have sufficient mechanisms in place to ensure that cards are returned and accounted for. … the return of ASICs issue will be addressed in these programs. DOTARS will also be auditing against these approved programs.
>
> Discussions with industry resulted in a number of approaches to achieving this outcome, all of which can be accommodated in the ASIC programs. SACL, for instance, favours requiring a bond for an ASIC and the Department supports this. Qantas, however, does not favour a bond system, and will demonstrate their mechanism for ASIC accountability through conditions of employment.

### Committee comment

6.31 Although in theory an expired ASICs can not be used, the high percentage of non-returned cards is of concern to the Committee. The reissue of ASICs and remodelling of ASIC programs will assist DoTaRS to respond to this issue. The Committee notes DoTaRS' advice that it will require ASIC programs to include mechanisms for ensuring the return of ASICs, and that the department will audit the performance of ASIC issuing bodies.

6.32 The Committee accepts that different ASIC issuing bodies should be able to determine the mechanisms to promote the return of expired ASICs which best suit their culture and operations. Notwithstanding this flexibility, if DoTaRS' audits reveal that the mechanism for the return of ASICs is inadequate, the issuing body should be required to change its procedures to address the problem.

### Recommendation 3

6.33 **The Department of Transport and Regional Services should set a performance standard for the return of expired aviation security identification cards (ASICs) for each card issuing body. If this standard is not met, the department should review the mechanisms for ASIC return in the issuing body's ASIC program and require change if considered necessary.**

6.34 During the inquiry, the Committee received other evidence *in camera* concerning the issuing of security passes, visitor passes and other access issues at a particular airport. The Committee has advised the authorities of any concerns that have arisen.

6.35 DoTaRS told the Committee that it was responding to the issues that were raised.[25]

## Trial of additional security procedures

6.36 The aviation security framework, underpinned by the legislation, permits aviation operators to introduce additional security measures. For example, Newcastle Airport Ltd (NAL) provided details of its trial of additional security measures for outbound domestic travellers. These measures require departing passengers to present photo identification together with their boarding passes at the screening point. Various provisions were also in place to enable adults and children without photo identification to transit the screening point. NAL estimated that the additional check took some 15 to 20 seconds if passengers were pre-warned of the requirements.[26]

6.37 NAL commented:

> NAL has devised this system to be simple, effective and easily implemented with the benefit of enhancing security at Newcastle Airport beyond that mandated by government regulations.
>
> The system has only minor implications for airline staff and only a small increase in workload applies to security screeners. Passengers have been overwhelmingly supportive of the initiative.[27]

6.38 DoTaRS advised the Committee that it had been monitoring the trial and had observed no adverse affect on mandated security outcomes. It noted that while people awaiting arrivals were unaffected, those farewelling departing passengers were not permitted into the sterile areas/departure lounge. DoTaRS added:

> Such restrictions as access to sterile areas were not adopted as part of the enhanced aviation security package announced in December 2003 and the Department has no proposals at this time to mandate

[25] Dr Andy Turner, *Transcript*, 24 November 2003, p. 28.

[26] NAL, *Submission No. 16*, pp. 93–4.

[27] NAL, *Submission No. 16*, p. 94.

> such measures, although all aspects of aviation security are under constant review.[28]

## Committee comment

6.39 Aviation participants should not consider mandated security measures to be all that is required of them. The aviation security framework permits participants to augment the prescribed requirements and participants should take advantage of this flexibility if they consider the additional security measure to be valuable.

6.40 Members of the Committee regularly travel to Newcastle Airport and agree that the additional measures are well received by the travelling public. The Committee commends NAL for its initiative.

# Security procedures at non-regulated airports

6.41 Although the Government has extended the coverage of Australia's aviation security regime,[29] many non-regulated airports remain. These airports remained unregulated because they do not service regular passenger aircraft.

6.42 The security at such airports is therefore not mandated, but determined by the airport operator. For example, Bankstown Airport told the Committee that it had installed a 'complete person-proof fence around the aircraft operating areas with appropriate security key pad gates.' This was despite being identified as being a low risk airport by a range of Commonwealth and State agencies.[30]

6.43 Bankstown Airport told the Committee of problems in ensuring security:

> We have in the past had some difficulty in convincing some of the longer standing tenants of the need to maintain that security perimeter, and we had no regulatory power to enforce that. Unfortunately, because we are not security categorised, there is no method under the Airports Act or the Air Navigation Act to enforce that.[31]

[28] DoTaRS, *Submission No. 79*, p. 437.

[29] DoTaRS, *Submission No. 79*, pp. 428, 454. A list of the airports to be included in the expanded regulatory system can be found at p. 460.

[30] Mr Kimber Ellis, *Transcript*, 2 October 2003, p. 41.

[31] Mr Kimber Ellis, *Transcript*, 2 October 2003, p. 41.

6.44 While the problem had been resolved, Bankstown airport recommended that there needs to be 'some form of power for airport owners or for the department of transport to enforce security measures where necessary.'[32]

6.45 DoTaRS responded to this issue with the advice that the matter could be 'addressed through contractual obligations and airport security program requirements.'[33]

## Committee comment

6.46 Arising from discussions during its inspection tour, the Committee understands that where regional airports are controlled by the local council, problems arising from uncooperative tenants do not occur. This is because council by-laws and tenancy agreements would ensure compliance with any security requirements.

6.47 Airports such as Bankstown, however, are not controlled by local councils. The Committee considers that DoTaRS' advice on this matter to be unhelpful because the security programs of non-regulated airports are not backed up by legislation.

6.48 It is possible for airports such as Bankstown to join the regulatory regime, but this would be likely to involve significant costs.[34] Alternatively, there may be relief through the provisions of occupational health and safety legislation. This is because security and safety are closely allied and a security measure can often be viewed in terms of maintaining a safe environment.

6.49 More generally, the Committee notes that other recently announced aviation security measures will strengthen security at non-regulated airports. These are:

- all pilots and trainee pilots will be subject to the same background checking process as used for issuing ASICs;
- pilots and trainee pilots will be issued with photographic passes from 1 July 2004; and
- general aviation aircraft will be required to implement anti-theft devices.[35]

6.50 The Committee recognises that these measures will place a financial burden on general aviation, but nevertheless supports this initiative.

[32] Mr Kimber Ellis, *Transcript*, 2 October 2003, p. 41.

[33] DoTaRS, *Submission No. 79*, p. 432.

[34] Mr Andrew Tongue, *Transcript*, 4 September 2003, p. 28.

[35] DoTaRS, *Submission No. 79*, p. 444.

# 7

# Training

## Introduction

7.1 While it is vital to have rules, procedures, and technologies in place, vulnerabilities will emerge if employees are inadequately trained to carry out those procedures. As the witness from Queensland Transport said:

> … some speakers from international security backgrounds mention that there has been too great an emphasis on the technological advances that we are making in aviation security and not on those relating to the human element not just in Australia but worldwide. … The provision of training programs and training techniques for all staff who come into contact with passengers needs to be, I think, a priority in the achievement of security outcomes. It is something that the airports, the regulator and the airlines—all parties who are playing a part in this solution—need to be mindful of.[1]

7.2 The inquiry did not cover the training or performance of customs, quarantine, and immigration officials, but instead focused on the training of private sector employees such as:

- check-in staff;

[1] Mr Damien Vasta, Queensland Transport, *Transcript*, 12 November 2003, p. 41.

- screening staff;
- cabin staff; and
- airport ground staff.

## Check-in staff

7.3 Check-in staff (often referred to as customer service agents) are predominantly employed by airline operators and are represented industrially by the Australian Services Union. The union told the Committee that the focus of security training had been on pilots, flight attendants and screeners.[2] The union commented:

> Our members include 33 of the overseas carriers, plus the major domestic and regional airlines. The inquiries I made do not indicate that there has been any specific additional security training.[3]

7.4 The Committee questioned the domestic carriers on this issue. Qantas responded that it was in the process of rolling out additional security training for all ground staff including customer service agents. Training included recognising unusual behaviour and training in conflict resolution. In both instances, however, the customer service agent was encouraged to alert their supervisor if incidents arose.[4]

7.5 Qantas later expanded on its comments, advising that the aim was to complete the training by the end of 2004. As well, since 11 September 2001:

> … all new customer service agents have received 90 minutes security training as part of their induction program. Additional training for the assessment of doubtful/unattended items have been given to all staff.[5]

7.6 Virgin Blue responded that its staff ‘had been trained as to security measures’ and it was continuously developing training programs. Training programs in accordance with ICAO standards had been submitted to DoTaRS. Virgin Blue’s staff had all been trained and had received specific training for their area of expertise.[6]

[2] Ms Linda White, ASU, *Transcript,* 21 October 2003, p. 40.

[3] Ms Linda White, ASU, *Transcript,* 21 October 2003, p. 31.

[4] Mr Geoffrey Askew, Qantas, *Transcript,* 12 November 2003, p. 13.

[5] Qantas, *Submission No. 74,* pp. 412–13.

[6] Mr Philip Scanlon, Virgin Blue, *Transcript,* 12 November 2003, p. 32.

## Screening staff

7.7 Screening is predominantly controlled by screening authorities such as the major airports and airline operators. The authorities employ security firms under contract to conduct screening. Screening staff are represented industrially by the Australian Liquor, Hospitality and Miscellaneous Workers Union (LHMU).

7.8 The LHMU raised several issues which it considered inhibited good security outcomes, including:

- the great variation in training and workforce standards between airports—the LHMU suggested a national system of accreditation was needed; companies were signing off on their training outcomes and there were a number of cases where minimum standards were not being met;
- the high levels of casual employees—experienced security officer LHMU members were concerned they had to continuously monitor the performance of poorly trained casual personnel;
- low wages and poor job security—this contributed to high staff turnover resulting in the loss of skills within the workforce;
- the use of labour hire security employees and sub-contracting by security firms—this should be prohibited; and
- the lack of training enabling guards to undertake extensive physical searches—a protocol was needed to establish who was responsible for undertaking this type of search.[7]

7.9 The LHMU's reiterated its comments when it appeared before the Committee.[8]

7.10 The three main security companies (Chubb Security Personnel, Group 4 Securitas Pty Ltd, and SNP Security) responded to the issues raised by the LHMU in submissions and at a subsequent public hearing. The responses were:

- Since 2000 there had been a national screener accreditation program which had to be obtained from a Australian National Training Authority registered training organisation. Screeners had to complete compulsory and elective modules of training, qualify for an ASIC, complete dangerous goods awareness training, and successfully

[7] LHMU, *Submission No. 12,* pp. 74–6.

[8] Mr Jeff Lawrence, LHMU, *Transcript,* 2 October 2003, pp. 63–74.

complete 40 hours one-to-one on-the-job training with a qualified work assessor. Screeners were subject to annual recurrent training.[9]

- Only a small percentage of casual staff were employed (some 3% by number, or 6% by hours worked)—they were needed to cover absences or fill four hour shifts. Many casuals worked regular daily shifts. They were required to meet the same standards as permanent employees.[10]
- Average annual earnings for a Chubb permanent employee was $38 000. Staff turnover for aviation security personnel was half that of other types of security employees (just less than 9% compared to just over 20% respectively).[11]
- Sub-contractors were used only in regional or remote areas—they were subject to the same training standards and quality assurance programs.[12]
- While Group 4 had insurance cover for issues arising from body / pat-down searches, there was no cover for individuals. Chubb had supported its employees in litigation concerning non-aviation security, but there needed to be some form of cover for individuals.[13]

7.11 Qantas also told the Committee that the average annual turnover rate for screeners employed by its contractors was 14.3 per cent. This compared with turnover rates of 12.9 per cent for Qantas staff and 18 per cent for screening staff in the USA.[14]

7.12 In a supplementary submission, DoTaRS provided more details of the training required of security officers:

> The Department has mandated that the screening of people, goods and vehicles is to be undertaken by people who hold the *Certificate II in Security (Guarding) with special application to Aviation Screening.* … Screener training is provided at the workplace by … ‘Registered Training Organisations’ … [which] must be registered with the State / Territory Registration Body under the Australian

[9] SNP, *Submission No. 69,* p. 389; Chubb, *Submission No. 65,* p. 371; Ms Alisa Goodyear, Chubb, *Transcript,* 24 November 2003, p. 12.

[10] SNP, *Submission No. 69,* p. 389; Mr Alexander George, Group 4, *Transcript,* 24 November 2003, p. 2; Chubb, *Submission No. 65,* p. 374.

[11] Mr Alexander George, Group 4, *Transcript,* 24 November 2003, p. 2; Chubb, *Submission No. 65,* p. 374.

[12] Mr Michael McKinnon, Ms Alisa Goodyear, Chubb, *Transcript,* 24 November 2003, p. 15.

[13] Mr Alexander George, Group 4, Ms Alisa Goodyear, Chubb, *Transcript,* 24 November 2003, p. 17.

[14] Mr Geoffrey Askew, *Transcript,* 12 November 2003, p. 9.

> Quality Training Framework … [which] comprises two sets of nationally agreed standards … [15]

## Private or public sector screening

7.13 Group 4 and Chubb raised the issue as to whether private sector or public sector entities should be responsible for providing screening services.

7.14 Group 4 argued that the competitive environment created pressure on the private sector screening companies to 'maintain quality or risk losing business to a competitor.' If services were provided by a government or quasi-government entity—where employment was 'pretty much guaranteed'—the lack of competitive pressure could result in a loss of competence or drop in standards.[16]

7.15 Chubb's submission stated:

> Recent surveys from the General Accounting Office of the USA point toward a deficiency in training, particularly recurrent and supervisory training, annual proficiency reviews, and annual certification programs. The interim reports have not been extremely favorable with many questions of quality still outstanding. It is also interesting to note that the TSA is currently running a pilot program in which they are assessing the possibility of returning the passenger screening function to private security firms.[17]

## Committee comment

7.16 The Committee is satisfied with the arrangements for the training of security screeners. The Committee notes that the April 2004 Draft Regulations cover the training and qualifications of screening officers. Screeners are required to hold 'at least a Certificate II in Security Operations'. For the first 40 hours they are to be 'supervised by a qualified screener' and must be assessed annually by 'a suitably qualified assessor of a registered training organisation'.[18]

7.17 The Committee believes it is important to have competent and well paid screening staff who remain in the job. Experienced screening staff are an asset.

[15] DoTaRS, *Submission No. 82*, p. 523–4.

[16] Group 4, *Submission No. 67*, p. 381.

[17] Chubb, *Submission No. 66*, p. 373.

[18] April 2004 Draft Aviation Transport Security Regulations 2004, Division 5.3, 5.05 (1), (4), p. 76.

7.18 The Committee also considers that the use of sub-contractors for screening has been satisfactorily addressed by the screening companies.

7.19 Turning to physical searches, the Committee considers that the *Aviation Transport Security Act 2004* clearly sets out the powers and limitations of screeners.

7.20 The legislation allows screening officers to request, but not require, the removal of **any** item of the person's clothing if it is considered necessary in order to screen a person properly. If the request is refused and the person refuses to be screened in a private room by an officer of the same sex, and if the refusal means that it is impossible to screen the person properly, 'the screening officer **must** refuse to allow the person to pass the screening point.'[19]

7.21 The April 2004 Draft Regulations also specify the training necessary for screeners to undertake physical searches.

7.22 The draft regulations require the initial one-to-one supervision of a new screener to include secondary screening duties including 'searching people with a hand-held metal detector or conducting physical searches.' The annual reassessment is also to include conducting 'limited physical searches of people.'[20]

7.23 The Committee considers it appropriate for the private sector to provide screening services. Competition as well as DoTaRS' mandated requirements and auditing will create pressure to maintain standards. The Committee reviews how performance is assessed in Chapter 8.

## Flight and cabin crew

7.24 The submission from the FAAA stated that while the ICAO was rewriting its *ICAO Cabin Crew Training Manual* to incorporate greater security responsibilities, 'the only group not required to demonstrate their safety and security proficiency to an internationally agreed minimum standard is cabin crew.'[21]

7.25 Mr Clive Williams also referred to ICAO guidelines commenting that cabin crews should meet international security proficiency standards and

[19] *Aviation Transport Security Act 2004*, Section 93 (1), (2), (5), pp. 80–1 (emphasis added).

[20] April 2004 Draft Aviation Transport Security Regulations 2004, Division 5.3, 5.05 (2), (4), pp. 76–7.

[21] FAAA, *Submission No. 34*, p. 254.

that all flight crew should attend security awareness training on a regular basis.[22]

7.26 The submission from Qantas indicated that additional security training for flight and cabin crew had been introduced.[23] Virgin Blue Airlines told the Committee that it had submitted training programs to DoTaRS in accordance with ICAO standards and that its staff including pilots and cabin crew had all been trained.[24]

7.27 The value of the new training was subsequently confirmed by the FAAA:

> A cabin crew training program specifically addressing hijacking and security issues is now in force. It took some time to get that training program in place; it was a big and complex issue. We were able to participate in the development of the program. The feedback we are getting from the crew is that they love it. They are saying: 'It's fantastic. This is what we've needed for so long.'[25]

7.28 The Committee considers that the issue of flight and cabin crew security training has been addressed.

## Airport ground staff

7.29 Airport ground staff include baggage handlers, cargo and freight handlers, cleaners, caterers, ramp staff and refuellers.

7.30 There are some 180 airports in Australia which service regular passenger aircraft. Before December 2003 only 38 of these airports were regulated. Changes announced on 4 December 2003, however, will result in all 180 airports being included in the regulatory regime.[26] A feature of regulation is that ground staff are required to carry ASICs. Consequently all staff working at those airports will require ASICs.

7.31 The Committee has considered the training provided to ASIC holders.

7.32 Brisbane Airport advised the Committee that it did not provide any specific security awareness training when ASICs were issued. The submission continued:

[22] Mr Clive Williams, *Transcript,* 5 September 2003, p. 58.

[23] Qantas, *Submission No. 17,* pp. 103, 104.

[24] Mr Philip Scanlon, *Transcript,* 12 November 2003, p. 32.

[25] Mr Guy Maclean, *Transcript,* 5 September 2003, p. 71.

[26] DoTaRS, *Submission No. 79,* pp. 428, 443.

> On application, there is a requirement for the applicant to sign that they have read and understood all the security provisions that are printed on the form. The consequences of non-compliance are also provided to them on the same form and we consider that their signature is sufficient proof that they are aware of their obligations. Additionally, we supply the opportunity annually for all airport staff to attend a security awareness briefing as part of our Emergency Exercise Program.[27]

7.33 APAM told the Committee that apart from an induction course when ASICs were issued it did not undertake much ongoing security training because it did not have the resources. It tried to maintain a security culture through signage and newsletters and patrols.[28]

7.34 SACL advised the Committee that:

> Each new ASIC applicant has access to the Sydney Airport specific a Security Awareness Guide … [which] provides details of safety and security requirements at Sydney Airport and gives ASIC applicants the information required to undertake a 'Security Awareness Test'. The test consists of multiple choice questions which are randomly selected from a computer database.[29]

7.35 Coffs Harbour Regional Airport (a currently regulated airport) told the Committee that it trained officers to meet safety requirements and to include basic, fundamental security measures would not be a great impost. It added, however, that it did conduct an induction program for any new employee of the companies operating at the airport. This program attempted to instil basic security awareness, such as reporting unattended luggage.[30]

7.36 The Committee notes that the regulatory regime requires aviation participants to develop transport security programs that:

> … demonstrate that the participant:
>
> - is aware of their general responsibility to contribute to the maintenance of aviation security
> - has developed an integrated, responsible and proactive approach to managing aviation security …[31]

7.37 Consequently, the Committee sought information from DoTaRS concerning whether the guidance material it was providing to assist the

[27] BAC, *Submission No. 83*, p. 527.

[28] Ms Pamella Graham, *Transcript*, 21 October 2003, p. 12.

[29] SACL, *Submission No. 84*, p. 529.

[30] Mr Bevan Edwards, *Transcript*, 2 October 2003, p. 35.

[31] DoTaRS, *Submission No. 79*, p. 454.

preparation of security programs included the need to develop security awareness training for ASIC holders.

7.38 DoTaRS responded that security awareness training was not currently mandated for all ASIC holders, but the 'issue may be considered in the context of the development and approval of transport security programs'. DoTaRS added that a broad ranging review of security training (not just for ASIC holders) was currently being canvassed with industry.[32]

## Committee comment

7.39 The Committee acknowledges that many ASIC holders will have attended specified security training because of the nature of their duties. A proportion, however, will not have received security training. The Committee considers that all airport workers should have a minimum awareness of security issues.

7.40 The Committee believes that the computer-based security awareness test offered by SACL to ASIC applicants suggests a cost-effective training instrument. It is unclear from SACL's submission whether this test is compulsory. The Committee considers it would be relatively easy to require those ASIC holders who had not received security training as part of their duties to successfully complete a computer-based security awareness test. This could be required when ASICs were issued and also on a regular basis, such as annually.

### Recommendation 4

7.41 **The Department of Transport and Regional Services should require aviation participants to include in their transport security programs compulsory initial and ongoing security awareness training for airport security identification card holders who have not received security training as part of their normal duties.**

[32] DoTaRS, *Submission No. 87*, p. 536.

# 8

# Auditing performance

## Introduction

8.1 Auditing performance is integral to the establishment of procedures and provision of training because it tests whether training outcomes are achieved and maintained. Incentives to meet performance standards are also important. In the aviation industry incentives usually take the form of penalties for under-performance.

8.2 The Committee has considered how the major aviation industry stakeholders conduct their audits and apply penalties. The stakeholders reviewed are:

- the screening services contractors;
- the airports and airlines; and
- the regulator, DoTaRS.

## Audits undertaken by screening service contractors

8.3 There are significant commercial imperatives for screening services to be of a high standard. Group 4 told the Committee that there was competition between the three screening contractors:

> I know full well that if I do not perform for my customers—the screening authorities—to the standard they expect, I will have both competitors breathing down my neck looking to take over the business. I think that what that does is enhance the outcome.[1]

8.4 In addition, the liability exposure of the screening service provider should the process fail was significant. Group 4 advised the Committee that it had insurance cover of $200 million for any one incident, and the cost was substantial. Group 4 added:

> Even with such insurance in place, this does not necessarily cover the entire risk, nor does it remove further liability from the supplier. Therefore, it is incumbent on the provider to ensure all operatives participating the aviation screening process are adequately trained and experienced.[2]

8.5 As a result security screening companies had a program of internal audit which extended to the performance of subcontractors.[3] Chubb told the Committee that its regular audits of screening points included more than a systems test—they included reviews of training records and spot assessments of staff.[4]

8.6 Chubb Security Personnel told the Committee that the disciplinary procedures for breaches by staff ranged from retraining for lesser breaches, to relocation from aviation screening work to elsewhere in the organisation for serious misconduct.[5] An example of serious misconduct was a failure at a secondary screening point.[6]

## Audits undertaken by airports and airlines

8.7 Like the security screening companies, airports and airlines have internal audit programs. The programs comprise audits of internal processes as well as contractor performance.

[1] Mr Alexander George, *Transcript*, 24 November 2003, p. 3.

[2] Group 4 Securitas, *Submission No. 67*, p. 379.

[3] Chubb Security Personnel, *Submission No. 66*, p. 375.

[4] Ms Alisa Goodyear, *Transcript*, 24 November 2003, p. 13.

[5] Mr Michael McKinnon, *Transcript*, 24 November 2003, p. 18.

[6] A passenger triggering a response at a walk-through screening machine is directed to a secondary screening point. The passenger has to successfully pass through this point, or be physically searched, before proceeding into a secure zone.

8.8 For example, APAM told the Committee that it assessed its screening contractor's training records to ensure compliance with all requirements.[7] APAM also conducted penetration tests:

> We focus on three key areas. The first, obviously, is the screening point. We also focus on our primary air side access gate for vehicles … We do tests there to make sure that they do the appropriate checks. We also do those checks through the cargo terminals. … we have an ongoing program of conducting those tests. When we see another area of weakness, we look at bringing in another testing regime.[8]

8.9 APAM advised that its contract with its screener included a key performance indicator system under which financial penalties could be invoked for under-performance. The principle areas covered were compliance with regulations; meeting standards during audits; and reporting certain categories of information.[9]

8.10 As well, if APAM discovered individuals not displaying their ASICs, the ASIC or the access it provided was suspended for a short period of time. This, APAM told the Committee, was its own initiative rather than a regulator requirement.[10]

8.11 BAC told the Committee that it audited the visitor log books of companies at Brisbane airport. Recently, the authority for a company to issue visitors passes had been withdrawn until it complied with BAC's requirements.[11]

8.12 BAC also carried out breach testing at the airport. Representatives explained that when its security staff attempted to breach a screening point they used 'test pieces' rather than actual weapons because to do otherwise would have been illegal.[12]

8.13 The submission from Qantas provided an overview of its inspection program:

> Each year on its domestic network, Qantas undertakes in excess of:
>
> - 400 screening point systems tests;
> - 140 audits; and
> - 730 access penetration tests.[13]

[7] Ms Pamela Graham, *Transcript,* 21 October 2003, p. 7.

[8] Ms Pamela Graham, *Transcript,* 21 October 2003, p. 55.

[9] Ms Pamela Graham, *Transcript,* 21 October 2003, p. 14.

[10] Ms Pamela Graham, *Transcript,* 21 October 2003, p. 16.

[11] Mr Edward McPheat, *Transcript,* 12 November 2003, p. 57.

[12] Mr Edward McPheat, *Transcript,* 12 November 2003, p. 59.

[13] Qantas Airways Ltd, *Submission No. 17,* p. 102.

8.14 Penetration tests could involve passenger screening points as well as freight terminals. Qantas gave an example of a penetration test:

> … one of our inspectors [would try] to get access to the apron through an open freight terminal, just walking from the road through the terminal. If they are able to access a security restricted area where they have not been challenged, we would say that we have undertaken an access control test and it has failed. … we would take that information to that airport operator or to that terminal operator and seek a remedy to that.[14]

8.15 Qantas subsequently provided details of the failure rates for its access penetration tests. Its submission stated that for 2002, some 7.3 per cent of the 730 domestic access penetration tests had failed. The failure rate for the 66 international penetration tests had been 12.1 per cent.[15]

8.16 Qantas told the Committee that if a screener failed to abide by a screening process, Qantas asked the contractor to move that person to a new site. If a skills test was failed, the contractor was asked to remove and retrain the screener before allowing him / her to return to screening.[16]

8.17 Qantas also had quarterly meetings with its three screening contractors with a view to benchmarking their performance.[17]

8.18 Virgin Blue told the Committee that it also audited the airports in its network and conducted access penetration tests. While the rate for successfully preventing penetration was not quantified, Virgin Blue commented that it was 'fairly high.'[18]

## Committee comment

8.19 The Committee is reassured by the evidence that aviation transport participants have self audit programs. Besides the duty of care responsibilities and potential liabilities arising from a major 'security incident', a significant motivation arises from the presence of the regulator. As APAM told the Committee:

> We audit a number of our processes because we know we are going to be audited by the department as well. We are always in a program of self-audit.[19]

[14] Mr Geoffrey Askew, *Transcript,* 12 November 2003, p. 17.

[15] Qantas, *Submission No. 74,* p. 413.

[16] Mr Geoffrey Askew, *Transcript,* 12 November 2003, p. 11.

[17] Mr Michael McKinnon, *Transcript,* 24 November 2003, p. 16.

[18] Mr Philip Geoffrey Scanlon, *Transcript,* 12 November 2003, pp. 31, 34.

[19] Ms Pamela Graham, *Transcript,* 21 October 2003, p. 55.

8.20 It is important, however, that the types of audit which are undertaken reflect the various threats which are likely to occur. In this regard the Committee was concerned to learn, when APAM briefed it on a serious breach at Melbourne Airport (see below),[20] that APAM's breach testing did not include people trying to sneak through a gate when no-one was looking.[21]

8.21 **The Committee expects that when DoTaRS assesses the proposed transport security programs of aviation participants, it ensures that internal audit programs reflect potential security threats.**

## Audits undertaken by the regulator

### Competency of Department of Transport and Regional Services staff

8.22 There has been criticism of the level of expertise of DoTaRS personnel.

8.23 Qantas commented that the restructuring of the Aviation Security Policy Branch had resulted in a 'loss of significant expertise'. It was vital, Qantas argued, that there be 'some security, airport, airline, aviation, law enforcement or similar operational expertise' to enable desired policy outcomes to be achieved.[22]

8.24 BAC and SACL expressed concerns similar to Qantas.[23] As well, Adelaide Airport commented that there lacked 'a suitable succession training program to retain expertise, or experienced personnel at the Executive or Head Office level.'[24]

8.25 The Committee asked DoTaRS to respond to Qantas' comments. The department responded:

> [The] comments tend to over-simplify the organisational change that has been affecting what is now the Office of Transport Security, and is a common feature of most organisations, including Qantas, at some stage in their evolution
>
> The twenty-two Aviation Security Regulation staff directly involved in aviation security compliance activities at this time,

[20] The incident occurred on 27 July 2003 and involved a passenger gaining access to the apron of Melbourne airport. *Transcript,* 21 October 2003, pp. 49–56.

[21] Ms Pamela Graham, *Transcript,* 21 October 2003, p. 55.

[22] Qantas, *Submission No. 17,* p. 107.

[23] BAC, *Submission No. 65,* p. 367; SACL, *Submission No. 15,* p. 89.

[24] Adelaide Airport, *Submission No. 18,* p. 120.

> both in Regional and Central offices, either have backgrounds of the kind referred to by Qantas, or have long standing experience working in the aviation security field. These backgrounds are appropriate for an organisation whose role it is to regulate, rather than to deliver, aviation security.[25]

## Training of departmental inspectors

8.26 The training provided to DoTaRS inspectors was criticised in a submission from Mr Christopher Smith:

> Aviation Security Inspectors continue to be tasked to inspect airlines and airports without the benefit of professional training in legislation, security programs or the audit process. … The lack of formal training often means valuable time is wasted clarifying the Branch priorities and policies. … Some suggest Inspectors should be able to assess threats and develop or analyse security procedures to counter the threat. Again this needs formal training and development.[26]

8.27 DoTaRS responded that it had long recognised the importance of a structured training program,[27] and it was currently developing manuals and guidance materials for the introduction of new auditing procedures in the second half of 2004 which would accompany the new regulatory framework. There would also be appropriate surveillance training for security inspectors.[28]

8.28 A theme in the evidence presented by the ANAO was that while DoTaRS had focussed on strategic issues it had been slow in implementing the ANAO's recommendations.[29]

8.29 This view is supported by the fact that it was in 1988 that the ANAO recommended that the then Department of Transport and Regional Development (DoTaRD) 'implement a training and development program to ensure that staff undertaking audits have formal training in security inspection and assessment techniques,' and 'develop operational guidelines outlining the policies, procedures and standards to be adopted

[25] DoTaRS, *Submission No. 87*, p. 538.

[26] Mr Christopher Smith, *Submission No. 73*, pp. 408–9.

[27] DoTaRS, *Submission No. 79*, p. 441.

[28] DoTaRS, *Submission No. 29*, pp. 212–13.

[29] Mr Warren Cochrane, *Transcript*, 4 September 2003, p. 6.

by all aviation security staff.' At the time, DoTaRD had agreed to the recommendation.[30]

### Committee comment

8.30 The Committee notes that the Government announcement on 4 December 2003 provided additional funding to enable the expansion of the aviation security regime and that a 'significant proportion of this funding would go towards a four-fold increase in the Department's resources to monitor industry compliance (i.e. auditors).'[31]

8.31 **The Committee expects DoTaRS to meet its commitment in regard to training and auditing manuals.**

## Types of audit performed

8.32 The ANAO criticised the sophistication of the audits undertaken by DoTaRS inspectors. Witnesses told the Committee that DoTaRS employed a product based approach where 'you take a check list and you look at what is happening' and mark off whether standards are being met. [32] The ANAO's submission added:

> … airport and airline audits varied in their thoroughness and rigor due to the varying quality of inspectors' inquiries and the lack of monitoring guidance for inspectors. … in the face of repeating security breaches DoTaRS inspectors may need to examine airport and airline procedures and to comment on any perceived deficiencies.[33]

8.33 DoTaRS agreed to ANAO's recommendation in the audit report that DoTaRS adopt a more systems based auditing approach.[34] DoTaRS advised the Committee that the new systems based auditing would commence 'in the second half of 2004 to coincide with the introduction of the new aviation security regulatory framework.'[35]

8.34 On the other hand, Mr Smith argued that inspectors should go beyond merely verifying that procedures applied by aviation participants conformed to the procedures described in their approved security programs:

[30] Auditor-General, *Audit Report No. 16, 1998–1999, Aviation Security in Australia, Department of Transport and Regional Services*, Canberra 1998, Recommendation 8, p. 23.

[31] DoTaRS, *Submission No. 79*, p. 442.

[32] Mr Michael Lewis, *Transcript*, 4 September 2003, p. 3.

[33] Auditor-General, *Audit Report No. 26, 2002–2003*, p. 45.

[34] Auditor-General, *Audit Report No. 26, 2002–2003,* Recommendation 2, p. 46.

[35] DoTaRS, *Submission No. 29*, p. 213.

> … there is folly in assuming that procedures developed during periods of low risk will be effective procedures during periods of high risk particularly when the procedures are developed by personnel with no understanding or experience of high risk. The same applies to regulatory inspection. Inspectors must be given the best training available to ensure they have the best understanding and experience of procedures for high risk situations. Some suggest inspectors should be able to assess threats and develop or analyse security procedures to counter the threat.[36]

8.35 DoTaRS responded that, contrary to Mr Smith's view, the primary role of the inspector was to focus on the compliance of procedures with the security program and that this 'role should not be blurred by seeking *ad hoc* application of additional provisions.'[37]

## Committee comment

8.36 The Committee accepts DoTaRS' view of the role of its inspectors.

8.37 Aviation participants are in the best position to formulate the measures applicable to their operations. They either have the expertise on their staff, for example APAM,[38] or are able to hire consultants with a knowledge and experience of high risk situations. Moreover, aviation participants will be in the best position to know what is practical in their operational environment.

8.38 In the assessment of transport security programs it is the expertise residing in DoTaRS Central Office which is critical. Security program evaluators will have the advantage of being able to compare and benchmark the security measures in the various security programs and with security programs in other countries.

8.39 Nevertheless, the Committee believes that transport security programs should contain contingency plans for an environment of increased threat. The Committee has noted in Chapter 6 that the use of regulations will allow a rapid response if the threat environment changes.

8.40 The Committee does not believe Australia's aviation participants are reluctant to devise appropriate security measures. While they are profit-making organisations, the Committee is confident that their duty-of-care, insurance liability concerns, and the potential losses arising from a 'serious security incident' are sufficient motivators. When breaches have

[36] Mr Christopher Smith, *Submission No. 73*, pp. 408, 409.

[37] DoTaRS, *Submission No. 79*, p. 441.

[38] Ms Pamela Graham, *Transcript*, 21 October 2003, p. 2.

occurred, participants have demonstrated their willingness to respond quickly—such as closing down a domestic terminal—thereby incurring financial loss and inconveniencing thousands of passengers.[39]

## Audits of airports and airlines

8.41 The ANAO audit concluded that the audits of airports and airlines were sufficiently frequent, well timed, and conducted according to schedule. It was noted that DoTaRS modified the timing of audits to ensure that a major airport was audited before any significant event, such as Sydney airport before the Olympics.[40]

8.42 Witnesses also commented on the frequency of visits by DoTaRS. Brisbane Airport Corporation commented:

> Our friends … from the department are, to praise them, a bit like the plague. They are out at the airport virtually every day of the week doing some sort of inspection systems testing.[41]

8.43 APAM added that if department inspectors were at the airport, they would bring to APAM's attention anything which they observed to be incorrect, and would undertake random checks of screening.[42]

8.44 While airport operators appeared satisfied with DoTaRS' audit process, Qantas considered the results should be disseminated to stakeholders. The airline argued that if there were audits of processes which affected the operations of carriers, those carriers should be advised of the outcome. Providing such advice, Qantas stated, would enable it to work with the government agency, the airport or terminal operator to improve the process.[43]

8.45 As noted in Chapter 5, DoTaRS has responded to this issue. The department advised that at ASC meetings, airport audit findings were generally discussed and DoTaRS' formal advice of the outcome of its airports audits were usually tabled.[44]

[39] Mr Geoffrey Askew, *Transcript,* 12 November 2003, p. 17.

[40] Auditor-General, *Audit Report No. 26, 2002–2003,* p. 34.

[41] Mr Edward McPheat, *Transcript,* 12 November 2003, p. 59.

[42] Ms Pamela Graham, *Transcript,* 21 October 2003, p. 11.

[43] Mr Geoffrey Askew, *Transcript,* 12 November 2003, p. 11.

[44] DoTaRS, *Submission No. 87,* p. 538.

## Audits of air cargo operations

8.46 International air cargo is managed through a regulated agents scheme. Regulated agents handle the air cargo under an approved security program. The agents have to screen cargo from unfamiliar consignors.

8.47 The ANAO found that DoTaRS' auditing of regulated agents was guided by an 'identified set of risk factors', but only a small number of agents had been audited. Instead DoTaRS relied on intelligence from within the industry to identify concerns about particular agents. DoTaRS had advised the ANAO that a lack of resources had prevented greater monitoring.[45]

8.48 The ANAO recommended that DoTaRS 're-examine the resources applied to, and the frequency of, auditing regulated agents' compliance with their International Cargo Security Program.'[46] The ANAO subsequently advised the Committee that DoTaRS had recruited additional staff , but that this was insufficient for the department to commence audits.[47]

8.49 Similar criticisms were also levelled in the submission from Mr Smith. The submission reiterated the lack of DoTaRS personnel, but added that the department had not taken advantage of regional aviation inspectors to audit regulated agents. Mr Smith cited an example where he was aware that a regulated agent was not following procedures and commented:

> Companies continually complain about competitors who disregard the regulations and see no improvement in either the level of regulation or the application of security procedures. … Regulated agents, who support the security program, need to be assured that their efforts are necessary or they will lose interest and redirect funding to other areas.[48]

8.50 The Committee asked DoTaRS to respond to Mr Smith's submission. The department advised that regional aviation inspectors had been used in cargo auditing functions, but 'given available resources and other aviation security priorities' their work had become focused on other areas. The regulated agents scheme was subsequently administered from Central Office using a systems-based approach.[49]

8.51 DoTaRS also noted that the creation of its Transport Security Division on 1 July 2003 involved:

[45] Auditor-General, *Audit Report No. 26, 2002–2003,* p. 35.

[46] Auditor-General, *Audit Report No. 26, 2002–2003,* Recommendation 1, p. 36.

[47] ANAO, *Submission No. 22,* p. 152.

[48] Mr Christopher Smith, *Submission No. 73,* p. 410.

[49] DoTaRS, *Submission No. 79,* pp. 441–2.

- reorganising to allocate increased resources to cargo security integrated across all transport modes; and
- redesigning work processes to incorporate the auditing of cargo related agents into the work programmes of regional offices.[50]

8.52 The Committee notes that the government announcement on 4 December 2003 included the provision of 'a four-fold increase in [DoTaRS'] resources to monitor industry compliance (ie auditors), including that of Regulated Agents.'[51]

8.53 While the discussion above applies to international cargo, the government announcement also indicated that the Regulated Agents Scheme would be extended to domestic air freight.[52] The Committee sought an update on progress from DoTaRS.

8.54 DoTaRS advised that is was:

> … finalising details of an audit program that will commence in March 2004 and result in 70 regulated agents being audited by [departmental] officers between March and June 2004. In the light of these audits the program will be fine tuned to form the basis of a continuous audit program. After July 2004 the audit program will be expanded to cover regulated agents handling domestic airfreight …
>
> The strategy to expand the regulated agents scheme will … include a targeted communications component designed to inform domestic air freight forwarders of the requirement for them to comply with the scheme.[53]

## Penalties for breaches

8.55 *Audit Report No. 26, 2002–2003* discussed various methods by which DoTaRS could encourage compliance of aviation stakeholders following audit. The ANAO noted that there was little difference in letters to airports and airlines 'regardless of whether they had committed (i) a serious breach or less-serious breach or (ii) a one-off breach or a series of repeat breaches' and did not aggregate breaches to apply increased pressure to comply.[54]

[50] DoTaRS, *Submission No. 79,* p. 442.

[51] DoTaRS, *Submission No. 79,* p. 442.

[52] DoTaRS, *Submission No. 79,* p. 447.

[53] DoTaRS, *Submission No. 87,* p. 537.

[54] Auditor-General, *Audit Report No. 26, 2002–2003,* p. 52.

8.56 The ANAO added in its submission that this 'standard letter' approach had 'the potential to be interpreted by industry as a tacit acceptance that a certain level of breaches would be tolerated.'[55]

8.57 As well, while the legislation and regulations provided for civil monetary penalties for breaches, such penalties had 'never been applied'. The ANAO concluded there was no graded system of penalties because the requisite administrative procedures were absent. There were also 'no practical enforcement mechanisms in between a warning letter and the cancellation of the security program of an airport or airline.' Cancellation would prevent and airport or airline from operating in Australia and so would in effect only occur in extreme circumstances. It was therefore not a good enforcement tool.[56]

8.58 The ANAO recommended that 'DoTaRS take a more strategic and coordinated approach to ensuring compliance' and incorporate:

> … administrative policies and procedures for introducing a pyramid of enforcement to correct non-compliance at the appropriate level in the chain of authority.[57]

8.59 In response to the ANAO's recommendation, the *Aviation Transport Security Act 2004* provided, by way of the regulations, for the introduction of a demerits points system. DoTaRS commented:

> A demerit point system defers the imposition of serious punitive measures. A clear warning system is set up so that industry and the regulator have an ongoing 'health-check' on the delivery of security outcomes, prior to resorting to punitive enforcement measures.[58]

8.60 The proposed demerits system received a less than enthusiastic response from the aviation industry, ranging from in-principle acceptance to strident criticism.

8.61 Chubb told the Committee that demerits was one way to construct key performance indicators. It was how they were used and the resulting corrective action which was the key:

> You need to make sure it is properly constructed in the first place and that accountability rests predominantly where the responsible person is. That may be the airline operator, it may be us as the

[55] ANAO, *Submission No. 22,* p. 153.

[56] Auditor-General, *Audit Report No. 26, 2002–2003,* p. 54.

[57] Auditor-General, *Audit Report No. 26, 2002–2003,* Recommendation 4, p. 56.

[58] DoTaRS, *Submission No. 70,* p. 393.

> employer, it may be the individual employee or it could be a combination of all of them.[59]

8.62 APAM expressed a similar view. While it did not have an issue with the concept, the concern was how it would be applied:

> For example, would the regulator issue demerit points at one airport, if they went air side and saw that somebody was not displaying an ASIC, and not do it at another airport? … Would it be applied against the security program holder or would it be applied against the individual who was infringing the system?[60]

8.63 APAM also noted that the regulations under the *Air Navigation Act 1920* allowed the department to prosecute, but this had to APAM's knowledge never happened.[61]

8.64 SACL also questioned whether a standardised approach could be established nationally. It added that a demerit points system had 'the potential to impact unfavourably on the insurance costs, share price and credit status of airports and airlines.'[62]

8.65 Qantas supported the use of penalties against organisations and individuals to promote an accountability-based security culture and improving compliance, but noted there were a 'myriad of practical problems' with such a system. It was concerned that the introduction of a demerit system was in response to ANAO recommendations. If so, it could be 'a case in which issues of public perception were driving regulatory processes, rather than achieving enhanced security outcomes.'[63]

8.66 Like Qantas, Perth Airport and BARA suggested the demerits system did not link to improving security outcomes.[64] BARA went further and suggested that a demerit system denied natural justice. It supported this view with the example of breaches involving ASICs issued by an airport operator to employees of **another** business at the airport:

> It is entirely unreasonable to expect airport operators to be responsible for the actions of other employers in policing their employees in relation to ASIC requirements. Yet if the employees … repeatedly breach the ASIC requirements, under the demerit points system, it is the airport operator which incurs the demerit

[59] Mr Michael McKinnon, *Transcript*, 24 November 2003, p. 19.

[60] Ms Pamela Graham, *Transcript,* 21 October 2003, p. 9.

[61] Ms Pamela Graham, *Transcript,* 21 October 2003, p. 9.

[62] SACL, *Submission No. 15*, p. 90.

[63] Qantas, *Submission No. 17,* p. 113.

[64] Perth Airport, *Submission No. 28,* p. 188; Mr Warren Bennett, *Transcript,* 2 October 2003, p. 55.

> points against its security program. No penalty will attach to the actual employer of the infringing employee.[65]

8.67 The Committee asked the LHMU whether individual employees should be penalised under a demerits system. The LHMU responded:

> It is the employer's responsibility to ensure that there is an appropriate system in operation, … Obviously there can always be human failings, but the major issue to address is the system of work. To the extent to which people are not trained well enough or they are not paid well enough or they have rostering systems that put onerous burdens on them, that is going to detract from security.[66]

8.68 The Committee sought comment from DoTaRS. At the Committee's first hearing in September 2003, the witness speculated on the reasons for the adverse reaction to the proposed demerits system:

> … demerit points provide, if you like, a running tab of how people are going. One of the concerns in the industry is that once we had a running tab it might be taken out of perspective, and I agree it could be taken out of perspective. There would not be that sense of proportion between minor incidents and larger incidents, people would just look at the number.[67]

8.69 At the Committee's final hearing in November 2003, DoTaRS acknowledged that industry had 'some legitimate concerns' about the proposed demerits system. The witness added that in the interests of completing the legislation and introducing the regulations, the demerits system had been 'taken off the table'. It remained, however, in the proposed legislation and the department was continuing to work with the industry on the issue.[68]

## Committee comment

8.70 The Committee agrees with the ANAO's view that DoTaRS 'should properly hold airports and airlines accountable and ensure that they in turn hold their contractors and employees accountable for security breaches.'[69]

[65] BARA, *Submission No. 3,* p. 18.

[66] Mr Jeff Lawrence, *Transcript,* 21 October 2003, p. 66.

[67] Mr Andrew Tongue, *Transcript,* 4 September 2003, p. 28.

[68] Mr Andrew Tongue, *Transcript,* 24 November 2003, p. 29.

[69] Auditor-General, *Audit Report No. 26, 2002–2003,* p. 49.

8.71 Taking as an example the actions of a security screener which leads to a security breach, the Committee notes the evidence that:

- the screener can be disciplined by the screening contractor;[70]
- the screening contractor can be financially penalised by the airport;[71] but
- while DoTaRS can penalise the airport, this has not occurred.[72]

8.72 In practice therefore, there is a break in the chain of accountability.

8.73 The Committee has considered BARA's argument that the absence of an accountability link between an airport and employees of a separate company can lead to a denial of natural justice. The Committee believes there is a link because:

- the airport has leverage over the separate company because it can review the issuing of ASICs to employees of the separate company; and
- in the last resort has recourse to Part 2, Division 3, Section 15 of the *Aviation Transport Security Act 2004* which makes it an offence to hinder or obstruct compliance with the transport security program of another aviation industry participant.

8.74 In conclusion, the Committee, like some witnesses, supports a demerits system in principle. This is because demerits can provide a graded response and engage the chain of security responsibility. It therefore can promote positive security outcomes. The system, however, needs to be properly constructed and administered. The Committee agrees with APAM that it is the application which is the key.

8.75 If a demerits system is to be credible and provide a compliance incentive for all in the aviation industry, it must be rigorously and consistently applied, and must provide a real penalty. Also, aviation participants subject to demerit must be capable and prepared to apply penalties 'down the chain of accountability.'

8.76 The Committee welcomes the advice from DoTaRS that it is consulting further with the aviation industry before a demerits system is introduced.

[70] For example, Chubb Security Personnel told the Committee it would reassign or retrain screeners who failed a test.

[71] For example, APAM told the Committee that financial penalties were applied to its screening contractors for under-performance.

[72] APAM told the Committee that it was unaware of any DoTaRS prosecutions arising from security breaches.

The Committee notes that alternative models have been suggested,[73] but has no view as to their value as alternatives.

[73] SACL suggested the NSW WorkCover system—Mr Ronald Elliot, *Transcript,* 2 October 2003, p. 15; Cairns Port Authority suggested a Civil Aviation Safety Authority system—Mr Ian Robinson, *Transcript,* 12 November 2003, p. 70.

9

# Aviation security culture

## Introduction

9.1 Australia’s aviation security system is based on a layered arrangement. Each layer, from check-in to aircraft cabin, has a probability of failure. Increasing the number of layers and increasing the security effectiveness of each of them significantly reduces the probability of a simultaneous failure. The fact that there have been security breaches in Australia, however, even on aircraft demonstrates that the overall risk is not zero. Thankfully, Australia has not witnessed the simultaneous failure of all the layers of aviation security.[1]

9.2 While it is possible to have leading edge technology, best practice procedures, high quality training and compliance procedures, the robustness of the security system still relies on the human factor—the security culture. All aviation industry participants have a security culture and would claim it is strong—the question is, are such claims justified?

9.3 The Committee has not the resources to study in depth the security culture of the various sectors of the aviation industry, but makes the following comments based on its own observations and the evidence presented to it.

[1] Even in the case of the attempted hijack of 29 May 2004, the cabin crew was able to contain the situation—although with the help of passengers.

The Committee believes, however, that its conclusions are applicable industry-wide.

## Security culture at small airports

9.4 The Committee has inspected facilities at two regional airports—at Coffs Harbour and Tamworth. Representatives from both airports and from Bankstown Airport also appeared before the Committee. The three airports represented, respectively: a regulated airport; a non-regulated airport servicing regular passenger aircraft; and a non-regulated airport which did not service regular passenger aircraft.

9.5 Coffs Harbour Regional Airport management told the Committee that it had a staff of four people and knew the employers at the airport fairly well.[2] This was an advantage:

> This being a small organisation, or a small community, everybody knows everybody else. Security and safety come together, and we are always conscious of strange faces and people in places where they should not be.[3]

9.6 Coffs Harbour told the Committee that it promoted a security culture through various means:

> We regularly run a terminal evacuation exercise and we take that opportunity to bring the security culture into it. … we ask that if a new employee of any company comes on line we also give them an induction, to cover ourselves under health and safety requirements but also just to give them a bit of sales talk, to introduce that culture that if you see a piece of unattended luggage you should bring it to someone's attention. I do not know how effective we are at that, because it has never really been tested, but we certainly try to keep it constantly in people's minds.[4]

9.7 The Committee asked whether there had been a major security breach at the airport. Coffs Harbour responded that there had been a person who had gained airside access, 'but he only got to the other side of the door before he was stopped.'[5]

[2] Mr Bevan Edwards, *Transcript*, 2 October 2003, p. 34.

[3] Mr Bevan Edwards, *Transcript*, 2 October 2003, p. 29.

[4] Mr Bevan Edwards, *Transcript*, 2 October 2003, pp. 34–5.

[5] Mr Bevan Edwards, *Transcript*, 2 October 2003, p. 35.

9.8 Similar evidence was provided by Tamworth Airport which told the Committee that it had a very stable workforce, most of whom had been at the airport for 13 or 14 years:

> Everyone gets to know one another around the place. If anyone wanders into an area where they should not be, they are normally challenged by the people who work there—simply because they have that safety and security culture. They are very protective of their own facilities; for example, Qantas have two large maintenance hangars and, if someone wandered into that hangar who was not known, they would be very quickly challenged by one of the staff members.[6]

9.9 Tamworth Airport agreed with the Committee when it suggested that the low risk facing the airport arose from its remoteness, the small number of people working at the airport and the small size of aircraft using the airport (jet aircraft do not fly regular services to Tamworth).[7]

9.10 Bankstown Airport only services general aviation aircraft and is not regulated. Management told the Committee that it had initiated security arrangements which were additional to that required of a non-regulated airport or for the level of risk identified for the airport. These included a person-proof fence with keypad locks, regular security patrols and a photographic identification pass system.[8]

## Committee comment

9.11 The Committee believes that smaller airports are likely to have a robust security culture. This is because the small number of employees working at such airports promotes a community attitude and allows strangers to be quickly identified. As well, there is likely to be a low level of aircraft activity at such airports which means that periods of risk are short and provides management with time to promote a security culture through training and other means.

9.12 The attitude of the airport management is also crucial, in particular, if it is prepared to initiate security requirements that go beyond the measures that are mandated.

[6] Mr Michael Dubois, *Transcript*, 2 October 2003, p. 39.

[7] *Transcript*, 2 October 2003, p. 40.

[8] Mr Kimber Ellis, *Transcript*, 2 October 2003, pp. 43, 45.

## Security culture at large airports

9.13 Airport managers are the initial focus for criticisms arising from a security breach. The vast majority of workers at large airports, however, are not employed by airport management. For example, Brisbane Airport Corporation employs 130 staff, yet issues ASICs for 7 000 other employees.[9] APAM told the Committee that it had a staff of 160, but was 'accountable for an airport that has roughly 10 000 employees.'[10]

9.14 Airport managers advised the Committee that they promoted a security culture:

- through internal audits to counter complacency and keep people on their toes;[11]
- through dialogue with the unions to convey a better understanding of the outcomes being sought; and
- by signage around the airport, poster campaigns, newsletters, induction training, committees, and incident debriefing forums.[12]

9.15 More specifically, SACL told the Committee it policed very heavily the practice of people using their ASICs to 'swipe other individuals' through electronically controlled doors.[13] APAM cited the instance when it discovered that occasionally escorted visitors making deliveries to the airport were left unsupervised at the loading dock. APAM responded to the situation:

> … we put in a process where, if the escort driver had to go back to the gate because there were a number of other escorts, they simply took the person back with them and they went back to the end of the queue. So there are processes to try to address those sorts of things, but security is always about human factors. I think we have very good processes and procedures in place, but occasionally people do not always follow them. We are fairly vigilant about doing something about that if we ever discover that is the case.[14]

[9] Mr Edward McPheat, *Transcript,* 12 November 2003, p. 55.

[10] Ms Pamela Graham, *Transcript*, 21 October 2003, pp. 12, 55.

[11] Mr Bevan Edwards, *Transcript,* 21 October 2003, p. 20.

[12] Mr Ronald Elliot, *Transcript,* 2 October 2003, p. 27; Ms Pamela Graham, *Transcript*, 21 October 2003, p. 55.

[13] Mr Steven Fitzgerald, *Transcript,* 2 October 2003, p. 20.

[14] Ms Pamela Graham, *Transcript,* 21 October 2003, p. 6.

## Security incident at Melbourne Airport—a case study

9.16 On 27 July 2003 an airline passenger was 'fairly lively and vexatious' during check-in. The APS was called to talk to him and eventually he was allowed to proceed. He passed through Customs and screening without incident, then broke the 'break glass' alarm at doors leading to the airport apron. He accessed the apron through another break glass alarm.[15]

9.17 When next seen, the passenger was getting out of a vehicle at the other side of the airport by a ground transport officer who told personnel in a crewing office. Central control was advised and the passenger (who by now was trying on uniforms in the crewing office) was monitored until the APS arrived. It took two calls to central control and some 35 minutes for the APS to arrive.[16]

9.18 The person who challenged and monitored the passenger was a Qantas employee. He told the Committee that he was not involved in the debrief and was only offered counselling four days after the incident. The passenger was admitted to the psychiatric hospital at Broadmeadows.[17]

9.19 In explanation, APAM advised there were a number of alarms activated at the time of the incident due, it was subsequently found, to a 'cabling problem'. The APS initially had responded to an alarm in the wrong area. Even if the APS officer had gone to the correct area, APAM commented, he may not have seen the passenger because of all the equipment in the area.[18] APAM also advised that while Qantas had participated in the debrief, it was Qantas' decision whether or not to include the person who eventually challenged the intruder.[19]

## Committee comment

9.20 The security incident at Melbourne Airport highlights various aspects of security culture, namely:

- the risks of complacency;
- the need for post incident monitoring;
- the risks of challenging intruders;
- the need to provide feed-back and support to all involved.

[15] Ms Pamela Graham, *Transcript*, 21 October 2003, p. 49.

[16] Mr Rob Lipman, *Transcript*, 21 October 2003, pp. 32–3.

[17] Mr Rob Lipman, *Transcript*, 21 October 2003, p. 36.

[18] Ms Pamela Graham, *Transcript*, 21 October 2003, pp. 49–50.

[19] Ms Pamela Graham, *Transcript*, 21 October 2003, p. 51.

### Complacency

9.21 APAM admitted that at the time of the incident there was a 'very high number of false alarms' and:

> Unfortunately, some of the staff in the coordination centre had lived with that for some time, and I do not think they had brought it to anyone's attention. ... The responses may have been affected because there was an assumption that things were false alarms rather than real alarms.[20]

9.22 APAM subsequently agreed with the Committee that maintenance procedures now recognise security as a priority.[21]

9.23 The Committee comments that the assumption that alarms were false exposed a serious flaw in the security culture at the time of the incident.

### Post incident monitoring

9.24 The incident at Melbourne Airport was initially contained and apparently resolved when the passenger was spoken to by the APS at the check in area. The security problem subsequently re-emerged some time later after the passenger had passed through Customs and screening.

9.25 The Committee did not ascertain whether there was a procedure in place to monitor people after an incident to ensure security issues didn't reappear, or whether the system was activated. The Committee acknowledges that informal procedures may exist, and whether it is activated is always a matter of judgement of those attending the incident.

9.26 Nevertheless, the fact that the APS attended the incident should have raised concerns. The Committee considers that it would have been sensible to advise people further along the chain about the incident so that someone in authority was aware of the presence of a potentially disturbed passenger. The Committee accepts that this may indeed have occurred.

### Challenging intruders

9.27 The Committee notes that the passenger was observed in a secure area by a ground transport officer who did not challenge the intruder, but instead referred the matter to someone else.

9.28 Challenging intruders is potentially risky,[22] but is relied upon by airport managers:

[20] Ms Pamela Graham, *Transcript*, 21 October 2003, pp. 49, 50.

[21] Ms Pamela Graham, *Transcript*, 21 October 2003, p. 53.

> We spend a lot of time trying to promote a security culture where people do challenge if it appears that somebody is not in the right place. The issue of safety implications for staff in doing so was raised at our most recent security committee. … as the airport operator, we depend a great deal on that sort of culture prevailing, because there just is not enough APS staff on the apron to take on that accountability. So the whole notion of challenging people is fairly important to our culture, and a number of staff do it.[23]

9.29 The Committee notes that challenging may take other forms. For example, a person who overhears comments which may have security implications could either challenge directly or report the incident to the authorities. In so doing the challenger risks criticism if the security concerns are not borne out.

## Providing feed back and support

9.30 In the Melbourne Airport incident the Qantas employee involved was not debriefed and was only offered counselling several days after the event—almost as an afterthought.

9.31 The Committee considers that everyone involved in a security incident should be provided with timely feedback and support.

9.32 All employees need to be encouraged to participate in a security culture. While it may be unnecessary for a particular individual to be involved in a formal post-incident debrief, their efforts should at least be acknowledged.

9.33 Employees who challenge should not be penalised if they are mistaken. This is because such disapproval will become widely known to the workforce and will discourage the challenge culture desired by airport managers. On the other hand, over-zealous employees need to have their behaviour modified, but through sensitive and positive counselling.

[22] On 24 July 1998 two police offers were fatally shot by a gunman who entered the Capitol building in Washington DC. The first officer challenged the intruder when he failed to walk through a metal detector; the second officer challenged the intruder inside the building. ERRI Emergency Services Report, *Shooting at US Capitol building*, 25 July 1998.

[23] Ms Pamela Graham, *Transcript*, 21 October 2003, p. 54.

## Engaging the public

9.34 The Committee has received evidence on different ways in which the travelling public can become involved in aviation security, such as through signage and posters.

9.35 Qantas has suggested, however, that general airport staff and the public could become actively involved in airport security through a neighbourhood watch style of organisation. In a paper delivered at the 2003 Crime Stoppers International Conference in Melbourne, a Qantas representative said:

> We accept and encourage 'neighbourhood watch' programs, why not 'airport watch'. … We need to promote a level of security awareness across the board. … it is essential that the public at large be alert and know what to do when witnessing unusual behaviour. The taxi driver must know what to do when he overhears a suspicious conversation in his cab. The cleaner must know what to do when he witnesses some odd behaviour or locates an item that is out of place. They should all know what to report and how to report it. It is essential that we get the message across to everyone that they all have a part to play in the security process.[24]

9.36 The attitude and behaviour of airport workers will also affect the attitude of passengers. For example, members of the Committee have favourably compared the attitude of Australian aviation security screeners, among others, to the attitude of overseas airport screeners.

> **Committee—** … my own experience internationally is that the culture in our airports is more user friendly than in the United States, which is appalling. Generally, it is more comforting for passengers than I would have thought anywhere in Europe. …
>
> …
>
> **Brisbane Airport Corporation—** I have even received letters from passengers … who have been to London or New York, saying the process here is such a great experience because (a) they know they are being checked and (b) the way we facilitated it is so easy compared to overseas.[25]

[24] Qantas, *Submission No. 77*, pp. 423, 424.

[25] *Transcript*, 12 November 2003, p. 58.

9.37 BAC also told the Committee that it annually surveyed its customers, stakeholders and contractors on its performance.[26] BAC later provided the Committee with its *Quality of Service Monitoring Report* for 2003. The Committee notes that the issues surveyed included passenger comments on waiting times in various areas, the 'quality of passenger search process', and the 'efficiency of passenger search process'.[27]

9.38 At a later hearing the Committee raised the example of the courteous behaviour of Australian screening personnel as a passenger being screened set off an alarm.[28] The Committee notes in this regard, Chubb's advice that some of its clients ask that it provide supplemental training to its screeners in the areas of customer service, conflict resolution and effective communication.[29]

## Committee comment

9.39 The Committee firmly supports the view that the public should become engaged with aviation security. Such engagement will assist the public to:

- understand fully the reasons for security and any enhanced security measures;
- accept the inconvenience of security procedures, thereby reducing frustration and the occurrence of airport rage; and
- gain an understanding of how to recognise potential security situations and how to respond appropriately in those circumstances.

9.40 The Committee is pleased with the friendly, yet firm, attitude of screeners in Australia. The alternative—belligerence, heavy handedness, and arrogance—as exhibited in some countries will not engage the public, and therefore will hinder security outcomes.

9.41 The Committee notes that in Australia screening services are provided by the private sector. In countries such as the USA the public sector provides screening services. The Committee draws attention to Chubb's criticism in Chapter 7 of the quality of service provided by screeners in the USA. The Committee's experiences would seem to bear out this criticism.

[26] Mr Edward McPheat, *Transcript*, 12 November 2003, p. 59.

[27] BAC, *Exhibit No. 13, Brisbane Airport Corporation Quality of Service Monitoring Report to ACCC, June 2003*, pp. 15–18, 21.

[28] *Transcript*, 24 November 2003, pp. 4–5.

[29] Chubb Security Personnel, *Submission No. 66*, p. 371.

9.42 The Committee believes that in the post 11 September 2001 environment passengers on board aircraft are likely to actively respond to a security incident. Other than in such extreme situations, however, response to security incidents should be left to trained professionals. Not only is this for safety and effectiveness reasons, but also to reduce the risk of compromising any legal proceedings arising from the incident.

9.43 While the Committee supports the creation of neighbourhood watch type organisations for airports, such organisations should not be extended into any form of vigilante group.

## Committee conclusion

9.44 As noted earlier, first rate equipment, training and monitoring does not guarantee a robust security culture. If the people operating the equipment and auditing performance have an inappropriate attitude then the effectiveness of security will be diminished.

9.45 The Committee suggests that a strong security culture requires an attitude which comprises:

- an awareness of, and alertness to security risks;
- a willingness to take the extra time needed to fully comply with security procedures;
- a willingness to take risks when confronted with security ‘situations’; and
- a willingness to take responsibility and be accountable when security situations arise.

9.46 The Committee firmly believes management has a crucial role in allowing the attitudes listed above to flourish. Staff must be allowed to take risks—imposing sanctions against people who take risks sends a message to fellow workers that such behaviour is unwelcomed by management. It leads to a risk-averse culture which is dangerous because it stultifies initiative. The skill of management is in achieving the appropriate balance between encouraging risk-taking on the one hand and discouraging recklessness on the other.

9.47 When a robust security culture is achieved it needs to be actively maintained. Currently this is done through compliance auditing which predominantly measures skills and observed behaviour. Falling short of the required standard is met with sanctions of varying severity.

9.48 The Committee believes that there is room to encourage and support the attitudes associated with a strong security culture. Moreover, the Committee believes this can be achieved without invoking some form of sanction.

9.49 The Committee considers there is sufficient expertise available for aviation industry participants to develop ways to measure the prevailing attitude of staff to security. The Committee suggests that the use of such attitudinal surveys may be valuable in developing and reinforcing appropriate security attitudes.

9.50 It is human nature when completing a survey to wish to respond with the ‘correct’ answer. Therefore surveys could be designed to indicate the sorts of behaviour that are expected when security incidents arise and which are consistent with a robust security culture. Such surveys would support those who have the right attitude and encourage the adoption of correct attitudes by others. When security risks appear, there would be a good chance that the appropriate response would be made quickly and the risk would be addressed before it developed into a more serious incident.

### Recommendation 5

9.51 **The Department of Transport and Regional Services should ensure that the security programs of aviation industry participants include educational instruments designed to promote an appropriate attitude to security and, through this, a robust security culture.**

Bob Charles MP
Chairman
23 June 2004

A

# Appendix A—List of Submissions

1. AACE Worldwide Pty Ltd
2. Bankstown Airport Ltd
3. Board of Airline Representatives of Australia
4. Department of Agriculture Fisheries and Forestry Australia
5. Australian Airports Association
6. Department of Foreign Affairs and Trade
7. Mr John G Hinde
8. Hervey Bay City Council
9. CSIRO – Commonwealth Scientific and Industrial Research Organisation
10. Australian Airports Association, South Australian Division
11. S3 Strategic Security Solutions
12. Australian Liquor, Hospitality and Miscellaneous Workers Union
13. Life Technologies Pty Ltd
14. Virgin Blue Airlines Pty Ltd
15. Sydney Airports Corporation Limited
16. Newcastle Airport Ltd
17. Qantas Airways Ltd
18. Adelaide Airport

19. Australia Pacific Airports Corporation (Melbourne and Launceston Airports)
20. State Government of New South Wales
21. Department of Defence
22. Australian National Audit Office
23. Cairns Port Authority
24. Mackay Port Authority
25. Albury City
26. Australian Security Identity Alliance
27. State Government of Western Australia
28. Westralia Airports Corporation
29. Department of Transport and Regional Services
30. Department of Immigration and Multicultural and Indigenous Affairs
31. Australian Federal Police
32. State Government of Tasmania
33. Australian Customs Service
34. Flight Attendants' Association of Australia
35. Mr Clive Williams, Australian National University
36. Dr Barry J Dowty
37. Australian Local Government Association
38. Dr Heather Parker
39. Mr Gregory Foulds
40. Mr Sam Richards
41. Mr Denis Vanzella
42. Mr Stephen Melis
43. Tweed River Seaplane Services
44. Mr John Funnell
45. Mr Wayne Harder
46. Dr David Baker

47. Mr David Toohey

48. Mr James A. Davey

49. Mr Stephen Robinson

50. Mr Stan Wright

51. Aerotec Queensland

52. Dr Michael Keating

53. Mr Henri Richard

54. Mr James Auld

55. Mr Sid Sidebottom, MP, Federal Member for Braddon

56. State Government of South Australia

57. Queensland Government Aviation Steering Committee

58. Australian Federal Police

59. Curtin University of Technology

60. Australian Customs Service

61. Australian National Audit Office

62. Australian Services Union

63. Qantas Airways Ltd

64. Office of the Federal Privacy Commissioner

65. Brisbane Airport Corporation

66. Chubb Security Personnel

67. Group 4 Securitas Pty Ltd

68. Australian Airports Association

69. SNP Security

70. Department of Transport and Regional Services

71. State Government of Victoria

72. Group 4 Securitas Pty Ltd

73. Australian Security International Systems Training (ASIST) Pty Ltd

74. Qantas Airways Ltd

75. Australian Pacific Airports Corporation (Melbourne)

76. Australian Federal Police

77. Qantas Airways Ltd

78. Virgin Blue Airlines Pty Ltd

79. Department of Transport and Regional Services

80. State Government of New South Wales

81. Department of Immigration and Multicultural and Indigenous Affairs

82. Department of Transport and Regional Services

83. Brisbane Airport Corporation

84. Sydney Airports Corporation Ltd

85. State Government of Queensland

86. State Government of Victoria

87. Department of Transport and Regional Services

88. S3 Strategic Security Solutions

89. Department of Transport and Regional Services

90. Australian Federal Police

91. Board of Airline Representatives of Australia Inc

# Appendix B—List of Exhibits

1. Mackay Port Authority
   *Presentation to House of Representatives Committee on Regional Air Services*

2. Australian Federal Police,
   *Memorandum of Understanding with DOTARS*

3. CFI Soaring Club of Tasmania
   *Correspondence between Mr Richard Doyle and Mr Boyd Munro*

4. Australian Liquor, Hospitality and Miscellaneous Workers Union
   *Campaign Material – Boarding Pass Message, Securing Our Airports*

5. Australian Services Union
   *Preliminary Survey Results – Zero Air Rage*

6. ToLife Technologies Pty Ltd
   *ToLife Technologies – Aviation Security*

7. Qantas Airways Ltd
   *"Video – Protecting the Spirit"*

8. Department of Transport and Regional Services
   *Information package on enhanced aviation security measures*

9. Qantas Airways Ltd
   *Information for Escorting Agencies*

10. Raven Alliance
    *- Focus on Civil Aircraft, Protection from the Terrorist MANPAD Threat- Briefing Transcript (11.02.04)*

*11.* Department of Transport and Regional Services
*High Level Group on Aviation Security, Terms of Reference and Membership*

*12.* Office of the Federal Privacy Commissioner
*Submission to the Senate Legal and Constitutional Legislation Committee: Inquiry into Terrorism Bills*

*13.* Brisbane Airport Corporation
*Quality of Service Monitoring Report to ACCC*

*14.* Sydney Airports Corporation Ltd
*Review of Aviation Security in Australia*

C

# Appendix C — Witnesses appearing at the public hearing

## Canberra, Thursday 4 September 2003

**Agriculture, Fisheries and Forestry Australia – Australian Quarantine Inspection Services**

Mr John Cahill, Executive Manager

Mr Robert Murphy, National Manager, Border

**Australian Customs Service**

Ms Gail Batman, National Director, Border Intelligence and Passengers

Mr Timothy Chapman, National Manager, Passengers

**Australian Federal Police**

Ms Audrey Fagan, Executive Director Protection

Federal Agent Stephen Jackson, General Manager Protection and Guarding

### Australian National Audit Office

Mr Oliver Winder, Deputy Auditor-General

Mr Warren Cochrane, Group Executive Director, Performance Audit Services Group

Mr Michael Lewis, Executive Director, Performance Audit Services Group

Mr Grant Caine, Senior Director, Performance Audit Services Group

Ms Karen Sutcliffe, A/g Senior Director, Performance Audit Services Group

### Department of Defence

Ms Margot McCarthy, Head Defence Security Authority

Lt Colonel Darren Kerr, Commanding Officer, Army Security Authority

Captain Simon Cullen, RAN Commanding Officer, HMAS Albatross

Air Commodore Mark Lax, A/g Deputy Chief of Air Force

Mr John Fletcher, Director, Property Services, Corporate Services and Infrastructure Group

### Department of Transport and Regional Services

Mr Andrew Tongue, First Assistant Secretary, Transport Security Regulation Group

Dr Andy Turner, Assistant Secretary, Aviation Security Policy

Mr Tom Grant, General Manager, Organisation Development and Corporate Secretary, Air Services Australia

Mr Michael Howard, Manager, Office of Security Risk Management,
Air Services Australia

## Canberra, Friday 5 September 2003

**Australian Customs Service**

Ms Gail Jennifer Batman, National Director, Border Intelligence and Passengers

**Australian Security Identity Alliance**

Dr Edward Lewis, Convenor

**Commonwealth Scientific and Industrial Research Organisation**

Dr Stephen Giugni, A/g Director ICT Research Centre

Dr Warren King, IMT&S Executive Chair

Dr Robert Floyd, Leader - Program Development, Secure Australia Program

Dr Neale Fulton, Principal Research Engineer

**Department of Foreign Affairs and Trade**

Mr Bryce Hutchesson, Assistant Secretary, Anti –Terrorism and Intelligence Branch

Mr Greg French, Assistant Secretary, Legal Branch

Mr Paul Smith, Director, Protection, Privileges and Immunities Section

Mr David Engel, Director, Indonesia Section

Ms Elizabeth Ward, Director, Business Facilitation and Secure Trade Section

Mr Damien White, Executive Officer, International Law and Transitional Crime Section

Ms Maria Poulos, Executive Officer, Chemical Biological and Conventional Weapons Section

Mr Robert John Nash, Assistant Secretary, Passports Branch

**Department of Immigration and Multicultural and Indigenous Affairs**

Mr Todd Frew, Assistant Secretary, Entry Branch

Mr Jim Williams, Assistant Secretary, Unauthorised Arrival and Detention Operations

Mr Graham Hanna, Director, Air and Seaports Policy Section, Entry Policy and Systems Branch

Mr Vincent McMahon, Executive Coordinator, Border Control and Compliance Division

**Department of Industry, Tourism and Resources**

Ms Patricia Kelly, Head of Division, Tourism Division

Ms June Murphy, General Manager, Market Access Group, Tourism Division

**Flight Attendants' Association of Australia**

Mr Guy Maclean, Manager Safety & Regulatory Affairs – International Division

Miss Carol Locket, OH&S Convener

**Strategic and Defence Studies Centre, Australian National University**

Mr Clive Williams

## Sydney, Thursday 2 October 2003

**Australian Liquor, Hospitality and Miscellaneous Workers Union**

Mr Jeff Lawrence, National Secretary

**Bankstown Airport Administration**

Mr Kimber Ellis, General Manager

### Board of Airline Representatives of Australia

Mr Warren Bennett, Executive Director

### Coffs Harbour Airport Administration

Mr Bevan Edwards, Airport Manager

### Federal Privacy Commission

Mr Timothy Pilgrim, Deputy Federal Privacy Commissioner

Mr Paul Armstrong, Director, Policy

### State Government of New South Wales

Mr Brendan O'Reilly, A/g Director General, Premier's Department

Mr John Schmidt, Deputy Director General Cabinet Office

Mr Gordon Dojcinovic, Inspector, NSW Police

Mr Kent Donaldson, Executive Director, Transport Safety, Ministry of Transport

Mr Alan Lidbetter, Manager Security and Emergency Management, Ministry of Transport

### Sydney Airports Corporation Limited

Mr Steven Fitzgerald, General Manager, Airport Operations

Mr Ronald Elliott, Manager, Security

Mr Christopher John Falvey, General Manager, Corporate Affairs

### Tamworth Airport Administration

Mr Michael Dubois, Business Development Manager

## Melbourne, Tuesday 21 October 2003

**AACE Worldwide Pty Ltd**

Mr Peter Julian Reid, Engineering Manager

**Australian Airports Association**

Mr Bevan George Edwards, Secretary, New South Wales Division, Regional Airports Representative

Mr David Rodney Piper, Deputy National Chairman

Mr George Joseph Vallence, Member

**Australian Services Union**

Mr Noel Stanley, Occupation Health and Safety Delegate at Qantas Airways Ltd, Melbourne

Ms Linda White, Assistant National Secretary

Mr Rob Lipman, Member

**State Government of Western Australia**

Mr Andrew Garret Gaynor, Acting Manager, Aviation Policy, Department for Planning and Infrastructure

**ICTS Technologies**

Mr Udi Bechor, Director of International Operations

**Melbourne Airport, Australian Pacific Airports Corporation (APAC)**

Ms Pamela Margaret Graham, Manager, Operations

**S3 Strategic Security Solutions**

Mr Paul Fox, Executive Director

Mr Jeffrey Robert Lauder, Director of Operations

**ToLife Technologies Pty Ltd**

Mr Moshe Maor, Managing Director

Mr Moti Meital, Senior Security Consultant

## Brisbane, Wednesday 12 November 2003

**Brisbane Airport Corporation**

Mr Stephen Goodwin, General Manager, Operations

Mr Edward Thomas McPheat, Security and Emergency Services Manager

**Cairns Port Authority**

Mr Ian Robinson, General Manager, Airport

Mr Philip Warwick, Security and Emergency Services Manager

**L-3 Communications Security and Detection Systems**

Mr Mark Knox, Product Specialist

Mr Stephen Meltz, Vice President – Asia Pacific

**Qantas Airways Ltd**

Mr Geoff Askew, Group General Manager, Security and Investigations

Mr Trevor Jones, Manager Security Policy and Planning

### State Government of Queensland

Mr Richard Conder, Deputy Commissioner, Queensland Police

Mr Andy Henderson, Chief Superintendent, Queensland Police

Mr Col Robinson, Director Passenger Transport Development

Mr Damien Vasta, Senior Adviser, Aviation

### Virgin Blue Airlines Pty Ltd

Mr Phil Scanlon, Head of Security Department

Mr John Jerome O’ Callaghan, Government Relations Adviser

## Canberra, Monday 24 November 2003

### Chubb Security Personnel

Mr Michael McKinnon, Executive Director, Chubb Security Personnel

Ms Alisa Goodyear, National Aviation Manager

### Department of Transport and Regional Services

Mr Andrew Tongue, First Assistant Secretary, Transport Security Regulation Group

Dr Andy Turner, Assistant Secretary, Aviation Security Policy

### Group 4 Securitas Pty Ltd

Mr John George, Group General Manager

D

# Appendix D—Inspection visits

## Tuesday 20 May 2003

### Inspection and briefing at Kingsford Smith Airport Sydney

Briefing by representatives of Sydney Airport Corporation Ltd:

- Mr Chris Falvey, Director Corporate Affairs; and
- Mr Ron Elliott, Manager Airport Security.

Inspection of facilities and procedures at Terminal 1 (International).

Briefing by representatives of Qantas Airways Ltd:

- Mr Michael van der Velde, Security Manger, National Operations; and
- Mr Neil Shackle, Business Manager, Sydney Airport.

Inspection of facilities and procedures at Terminal 3 (Qantas domestic).

# Wednesday 1 October 2003

## Inspection and briefing at Tamworth Airport

Briefing by:

- Mr James Treloar, Mayor Tamworth;
- Mr Michael Dubois, Business Development Manager, Tamworth City Council;
- Mr Philip Lyon, General Manager, Tamworth City Council; and
- Mr Chris Durkin.

Inspection of facilities and procedures at Tamworth Airport.

## Inspection and briefing at Coffs Harbour Airport

Briefing by:

- Mr Bevan Edwards, Manager, Coffs Harbour Airport; and
- Mr Vaughan Jones, Managing Director, Coffs Coast Jet Centre.

Inspection of facilities and procedures at Coffs Harbour Airport.