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.