Australian Government

Airport Security and Policing Review

An Independent Review of Airport Security and Policing for the Government of Australia

by
The Rt Hon Sir John Wheeler DL

September 2005

ISBN 1 921092 15 7

Preface

On 5th June, 2005, the former Deputy Prime Minister and Minister for Transport and Regional Services, the Hon John Anderson MP, invited me to Head this Review into Airport Security and Policing. I subsequently liaised with the Department of Transport and Regional Services Secretary, Mr Michael Taylor, on the Terms of Reference for the Review and I have been engaged on the project since 7th June. My Review Team and I have visited a number of airports in Australia and it is upon the basis of these visits, research undertaken, the written submissions received and the detailed discussions that we have had, that I have developed my recommendations.

My approach to the Review has included taking a fresh look at the decisions already made by the Australian Government, especially those of recent months. Thus, I support and comment upon matters such as the proposed appointment of the Airport Security Controller and the role of CCTV. I have approached the issues relating to the safety and security of airports by reviewing the threat and risk from terrorism and crime and seeking to improve flows of relevant information. In addition, I have sought to improve the overall command and coordination structure and to enhance confidence building among Federal, State and relevant commercial interests. I have also made observations to improve essential aspects of security, including as they relate to the Aviation Security Identification Card (ASIC), airport access, cargo, and differences between the major airports and smaller centres.

I have been fortunate to have had the support of two able and energetic colleagues who have brought between them a range of talents and experiences entirely relevant to the issues. I pay a warm tribute to Mr John Abbott CBE QPM, formerly Director-General of the United Kingdom National Criminal Intelligence Service, and Mr Neil Fergus who had a distinguished career in public service, including managing security intelligence for the Sydney Olympics.

My review colleagues join with me in thanking the Head of the Review Secretariat, Mr Kym Bills for his able direction of the Review and the other members of the Review Secretariat who were: Dr Andrew Turner, Dr William O'Malley, Mrs Jane Hanna, Ms Gabrielle Crick, Mr Scott Shearer, Mr Kevin Luke, Ms Jill Brooks, Mrs Kay Hart, Ms Carolyn Shelper, Ms Erin Cann, Mr Hamish Hansford and Mr Daniel O'Malley.

THE RT HON SIR JOHN WHEELER
September 2005

Table of Contents

Terms of Reference

International expert review of security and policing at Australian airports

Noting the substantial measures the Australian Government has adopted to strengthen aviation security since the events of 11 September 2001, including passage of the *Aviation Transport Security Act, 2004*, additional resourcing and the significantly expanded roles and functions of several Australian Government agencies, and additional decisions taken on 7 June 2005, and also being aware of community concerns about criminal activity at Australian airports, the terms of reference for the inquiry are:

- To review the threat from serious and organised crime at airports and related cargo areas within Australia, taking into account any relevant reviews of criminal intelligence and the role of the law enforcement agencies
- To make recommendations on strengthening the integration of ground based aviation security and law enforcement arrangements, including through enhanced threat and risk assessments and whole of government response strategies
- To review the adequacy of current Australian ground based aviation security requirements and arrangements put in place in response to threats of terrorism, including in relation to
    - The Aviation Security Identity Card scheme and related aspects of background checking
    - Airport access controls
    - Scrutiny of airport workers and others entering the airside areas of major airports
    - The effectiveness of protective security co-ordination arrangements at major Australian airports
    - Security compliance of airports and airlines
    - Adoption of emerging technologies to mitigate security risks and related matters
    - International developments
- To make recommendations regarding roles and responsibilities, including the need for any legislative change and any related matters.

7 June 2005

Executive Summary

1. The safety and security of the people of Australia is the first duty of the Australian Government. The public has an exceptional sensitivity to aviation and airport security and a concern that criminality may lead to vulnerabilities that could be exploited by terrorists.

2. Airport security is both broader and narrower than aviation security as defined under the international standards and recommended practices represented by Annex 17 to the Chicago Convention by members of the International Civil Aviation Organization (ICAO). While a principal aim of airport security is to prevent 'unlawful interference' with aircraft that could lead to fatalities among passengers and crew, major airports themselves are critical infrastructure for the ongoing health of the economy and for people's lives and livelihoods, and are potential targets for serious crime and terrorism.

3. In Australia, exports and imports of $70 billion (8 per cent of Australia's GDP) pass through airports, and annual passenger arrivals and departures total some 100 million, of whom international passengers comprise 20 million. Airports also provide direct employment for about 150,000 Australians. Such flows of wealth and people through concentrated nodes provide rich opportunities for both crime and terrorism.

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

5. Terrorists also require funding for their operations and often engage in theft, fraud or drug trafficking. The 2004 theft by the Provisional IRA of 24 million pounds from a then Australian-owned bank in Belfast is a recent international example. Terrorists may raise funds by selling their expertise to organised criminals. This may occur in reverse, with major criminal gangs from time to time selling their expertise to terrorist groups, perhaps through intermediaries.

6. Experience around the world has demonstrated that airport policing and security is a specialist field requiring dedicated and trained officers, integrated systems, appropriate technology, and real partnerships between federal and state agencies and relevant private sector personnel. The submissions to the Review by the NSW Police, QANTAS and others have reinforced the importance of such an approach for major airports such as Sydney.

7. The Australian Government, State and Territory Governments and the private sector have made many positive security changes and have dedicated significant resources to combating terrorism, especially since the attacks in the United States on 11 September 2001. This three-month Review of airport security and policing commissioned by the Australian Government on 7 June 2005 has provided an opportunity to take a fresh and independent look at the measures introduced and whether there are any improvements that could usefully be made.

8. The Review was impressed by many of the measures taken in Australia since 2001 and heartened by the additional actions proposed and agreed during the Review's course. The lessons demonstrated by 'London resilience' in the aftermath of the terrorist bombings on 7 July 2005 provided a clear impetus to do even better. Based on its Terms of Reference, the focus of the Review was therefore to recommend actions, roles and responsibilities that could further improve the effectiveness and resilience of the systems at airports designed to maintain the security of Australians and their guests.

9. Seeking to understand the causes of terrorism and to combat the promulgation of strains of religious extremism and aberrant ideology, especially among young people, that lead to terrorist acts is a major priority for security services in Australia and internationally. Australia has developed a National Threat Assessment Centre within ASIO and established a network of liaison officers at major airports. However, sharing of information and intelligence assessments with appropriately cleared members of the police and private sector should be further improved, and aviation and airport-specific assessment material is less frequent than it could or should be.

10. Despite a current reference to the Australian Crime Commission (ACC), and some excellent one-off investigations by the Australian Customs Service (ACS), the Australian Federal Police (AFP) and State and Territory Police, there is no ongoing

mechanism to draw together and assess regularly the threat of crime and criminality at major airports. This new role would best be performed by the ACC and will require Customs, the AFP and State and Territory Police consistently to input timely data into the Australian Criminal Intelligence Database (ACID). Bringing together the streams of national security and crime intelligence and other information in a form needed by airports and transport industry operators will require a significantly enhanced capacity within the Office of Transport Security (OTS) in the Department of Transport and Regional Services (DOTARS).

11. The Review's Terms of Reference note the community concern about criminal activity at Australian airports and require a review of the threat and risk from serious and organised crime taking into account criminal intelligence and law enforcement roles. The Review had great difficulty in obtaining comprehensive airport crime data. That which exists relates to reported crimes which appear to be static or declining. However, there is a culture of under-reporting and tolerance of theft at airports and related cargo areas, and police are rarely on site to receive a report. Intelligence material, particularly from Customs, confirmed significant threats and vulnerabilities at major airports that are consistent with the reporting by *The Australian* on 31 May and 1 June 2005 of the unauthorised release of a classified Customs staff-level assessment at Sydney Airport.

12. Policing at major airports in Australia is often inadequate and dysfunctional, and security systems are typically uncoordinated. The roots of this include bureaucratic turf protection and unresolved Commonwealth/State conflicts over resources. To ensure policing is adequate and coordinated, the recently announced AFP Airport Security Controller positions should clearly be Airport Police Commanders, who may be seconded from well-qualified State and Northern Territory police for a five-year term.

13. The reason for this is that policing at an airport is a special skill for which all officers involved need to be appropriately trained so that they can deliver the full range of policing services. Such policing services are not confined to counter terrorism and the reactive investigation of so-called 'community policing' incidents. They should also include the proactive prevention, investigation and detection of serious, organised and volume crime and other offences, the maintenance of the peace, public reassurance, and ensuring public safety (with a particular emphasis on the capability to respond professionally to a major incident or emergency).

14. The Review recommends a minimum level of police numbers at the (currently eleven) Counter-Terrorism First Response (CTFR) airports. This is likely to require refinement of initial AFP cost estimates on the basis of consultation with the relevant jurisdiction's Police force and subsequent threat and risk assessments by each Airport Police Commander.

15. Airport Police Commanders should command all police functions at the airport inclusive of a specially trained 'ring-fenced' State or Territory Police contingent, as well as the Australian Federal Police Protective Service (AFPPS). For this model to be effective it will be essential for ring-fenced funding to come from the Commonwealth to the State or Territory for the required officers and other personnel. Police officers selected by Commanders from the State or Territory would continue to wear the uniform of their Police force and would receive pay and all conditions of service from their parent organisation and seek leave, promotion or reassignment in the normal way.

16. The Airport Police Commander must also be kept informed of any significant operations at the airport by Customs, Immigration, AQIS, ASIO, State or Territory Police and other agencies. If legislation and privacy guidelines currently prevent sharing of security-related information, changes must be made: such constraints do not apply to terrorists and criminals. The Commander's role must be clearly specified including in national Counter-Terrorism arrangements with simplified handover procedures to State and NT Police (and potentially to the Australian Defence Force). All police, AFPPS and Customs officers at airports need clear and unambiguous powers to stop, search, detain and arrest where necessary within the airport and its curtilage.

17. Airport Security Committees (ASCs) vary in size, seniority and effectiveness at major and regional airports. A more strategic ASC should be established at the major airports, with a core membership of the airport operator and key police, government agencies and industry representatives. This ASC should be focused and chaired by the airport CEO to enable in-depth discussion and ownership of security issues and the coordinated undertaking of airport-specific and enhanced multi-agency threat and risk analysis. A larger consultation group would be subsidiary to the ASC. Despite recent initiatives, Australia appears to be lagging behind leading Western countries, such as the UK, in integrating intelligence exchange between the public and private sectors, and this requires a significant mindset change and practical action.

18. The present Aviation Security Identification Card (ASIC) system has a number of weaknesses, and there is confusion as to what airport access an ASIC enables. Some weaknesses are already being addressed but additional steps are required. While the politically motivated violence (national security) checking system through ASIO is 'live' or ongoing, the criminal checking regime relies on convictions in a database at a point in time for the issuance of a two-year card. Subsequently recorded convictions are not automatically alerted, and applicants with a pattern of criminality or with major criminal associations are not potentially denied access. The checking process can take weeks to complete, causing unacceptable reliance on procedures for visitor cards which do not require background checks. There are 188 ASIC databases and authorising bodies around Australia and these are neither consistent nor linked. Some casual or contract workers, such as security screeners and cleaners do not initially hold ASICs and may not always be accompanied on-the-job by an ASIC holder as required under current legislation.

19. A new national card-authorising body within the Attorney-General's Department is required to bring together the national security and criminality streams and immigration checks on a timely 'live' basis and to apply judgements as to who is a fit and proper person for the purposes of access to sensitive airport areas and aircraft. Appeals against decisions of this body should be to a special section of the Administrative Appeals Tribunal as is currently available with respect to ASIO decisions. Employers also have a responsibility to screen prospective staff carefully before seeking an ASIC and to monitor any relevant behaviour after issue. This improved aviation system has a clear analogue in the maritime sector.

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

21. Regional airports and general aviation present particular challenges to security in an environment where 100 per cent security is never possible and where regional and remote Australians rely on aviation to maintain accessibility, employment and living standards. While principles should be consistent and based upon compliance with ICAO Annex 17, it is clear that 'one size does not fit all' in imposing security, regulations and standards across disparate airports. For example, airport fencing is a very temporary deterrent and, despite its expense, does little to protect the sensitive aircraft apron and airport terminal areas. Security measures at regional airports should be balanced and proportionate and must be based on enhanced threat and risk assessments. It is always difficult to draw firm lines, and these could vary as a result of changed circumstances. Nevertheless, in the current environment, consideration should be given to more comprehensive security control over regional flight passengers when arriving at major airports such as Sydney because of the risk to larger aircraft and facilities when passengers disembark at the apron.

22. The licensing of security personnel varies across jurisdictions and training given to staff such as screeners is less adequate than in countries such as Singapore, and should be enhanced. This should occur as part of a more comprehensive training programme for all security-related airport staff as required under Annex 17. Improved screening is an appropriate defence to help mitigate risks associated with the increasing use of self-service ticketing where passenger identity cannot be certain.

23. For many regional airports, a major improvement in security systems, awareness and risk management would be achieved through an enhanced security promotion and assistance role undertaken within the Office of Transport Security in DOTARS. This should include education in best practice, help in understanding regulatory requirements, basic security training, and assistance in preparing documentation required to access further programmes and resources. Additional assistance with physical infrastructure security guidance should be provided by ASIO's T4 to major CTFR airports and other airports that require it. Cost recovery should not be allowed to inhibit necessary security improvements, and Commonwealth assistance with costs will therefore be required.

24. The *Aviation Transport Security Act 2004* provides a solid basis for security regulation of airports and associated activities. The *Act* and the *Aviation Transport Security Regulations 2005* were,

however, developed with less than optimal consultation in order to be operative from 10 March 2005 and would benefit from a review with the aim of clarification and simplification. There is a danger that airport security could become focused on compliance with regulations rather than on the crucial preventative role through assessing threat and risks on an ongoing, involving and consultative basis and mitigating these in a timely way. Regulation should encourage good outcomes through good systems and processes and through improved behaviour and culture.

25. While 80 per cent of Australia's air cargo is carried on passenger aircraft, it is not all screened. It is clearly inconsistent for one category of aircraft user to be treated differently from another, thereby putting the safety of the aircraft in jeopardy. Cargo should be screened on all aircraft where check-in baggage is screened in order to reduce the risk of explosives being placed on board through the freight system.

26. Developing technology such as the Customs trials of neutron scanning and Smartgate are good examples of potentially significant advances. Timely assessment of emerging technologies, more generally, is essential for Australia to have proven leading-edge airport security. This should be coordinated through the enhanced role of a Commonwealth body such as the Department of the Prime Minister and Cabinet's Science, Engineering and Technology Unit.

27. The National Security Committee of Cabinet is the Australian Government's primary forum to address aviation and airport security and broader national security issues. The Review agrees with the Government that this Committee has worked increasingly well, particularly since the Bali bombings in 2002. It is this Committee which should assess progress with implementation of the recommendations made by this Review based on the advice of the Cabinet Implementation Unit.

28. The Review believes that the fine tuning, further measures, and clearer roles it proposes will enable a balanced and achievable improvement to Australia's airport security and policing. However, further major gains will require a changed culture of cooperation, sharing, and openness to new technologies and methods across Federal, State and private sector agencies and personnel, in order to replace the silos and insularity which continue to provide unnecessary weaknesses that could be exploited by criminals and terrorists.

Recommendations

I. It is recommended that a thorough examination of legislation and regulations on the sharing of information, both among government agencies and between government and the private sector, be carried out by the Attorney-General's Department, in collaboration with States and Territories and the private sector, with the aim of identifying and removing elements which prohibit or inhibit the flow of information needed to counter crime and terrorism which threaten the aviation sector.

II. It is recommended that the National Threat Assessment Centre prepare and distribute general national security Threat Assessments on the dangers posed to aviation and airports on a regular basis, and at least quarterly.

III. It is recommended that there be established within the Australian Crime Commission a unit on aviation and airport criminality to collect, collate, and analyse relevant information on criminal behaviour, and to produce regular reports, including Criminality Assessments at least quarterly.

IV. It is recommended that the Security Analysis Section within the Office of Transport Security in the Department of Transport and Regional Services be given additional analytical and reporting capability. Its tasks should include producing regular reports on security issues facing Australia's aviation industry and airports and to disseminate them in a timely fashion to those in the industry with a need to know, with a reciprocal feedback loop. This model is likely to be applicable to Australia's maritime and land transport industries.

V. It is recommended that criteria be established to determine under what conditions an airport should become or cease to be a Counter-Terrorism First Response airport, and that the Department of Transport and Regional Services be required to review CTFR airports and the major non-CTFR airports on a regular basis and at least once every three years so as to determine whether their classification is appropriate.

VI. With regard to policing at airports, it is recommended that:

- the position of Airport Police Commander be established at each CTFR airport, to be filled by a senior police officer holding appropriate rank in the Australian Federal Police but who may be seconded from a State or Territory force. The Commander's responsibilities will be to command the

general policing presence, which will include the delivery of all policing functions such as public reassurance and prevention, the proactive and reactive investigation of crimes and offences, keeping the peace, as well as deterring and responding to terrorism

- the Airport Police Commander be selected by a panel including the AFP and the Police force in the jurisdiction in which the airport is located
- the Airport Police Commander work in collaboration with other government agencies assigned to the airport, and supervise the work of an appropriately staffed Joint Intelligence Cell
- an appropriately sized State or Territory Police contingent be posted to each CTFR airport, and comprise police officers selected by the Airport Police Commander and specially trained for airport duties and assigned solely to tasks at the airport
- all police, AFPPS and Customs officers deployed to an airport be given clear and unambiguous powers, including to stop, search, detain and arrest where necessary within the airport and adjacent roads and parking areas
- the Commonwealth provide ring-fenced funding for all policing functions at CTFR airports which includes the CTFR function and the general police presence
- legislation be reviewed to provide appropriate powers.

VII. It is recommended that the Department of Transport and Regional Services require that the Airport Security Committee be refashioned at each CTFR airport to be a focused and strategic group, chaired by the CEO of the airport or the CEO's high-level representative. Its members, including the Airport Police Commander, are to be security cleared representatives of government agencies and major operators with security interests at the airport. Its tasks are to identify security threats and risks and to initiate action to address them and to monitor their implementation. The current larger existing Airport Security Committees at CTFR airports should be renamed Airport Security Consultative Groups.

VIII. It is recommended that the Department of Transport and Regional Services require that Transport Security Programs be supplemented by a more frequent system of reporting that ensures that airports regularly review their own security gaps

and weaknesses and document the measures being taken to address them. Reviews of threat and risk should be undertaken by Airport Security Committees, with their reports collected and analysed centrally by the Office of Transport Security in DOTARS, in order to bolster the national effort to understand and counter threats.

IX. It is recommended that the *Aviation Transport Security Act 2004* and the 2005 Regulations be reviewed by the Department of Transport and Regional Services to ensure that they encourage a culture of proactive and ongoing threat and risk assessment and mitigation and not a passive culture of compliance.

X. It is recommended that the background checking process required to obtain and hold an Aviation Security Identification Card be further tightened and centralised in the Attorney-General's Department and that this should be harmonised with maritime cards.

XI. It is recommended that integrated Closed-Circuit Television systems be expanded and improved at Australian airports, and that, with the Australian Customs Service as the lead agency, arrangements be made to ensure CCTV standardisation, digital upgrading, storage, and fully coordinated use by Customs, police and security personnel.

XII. It is recommended that the Attorney-General's Department work with State and Territory Governments to require that private security officers in the aviation industry, including those responsible for screening at airports, be background-checked, licensed, and trained to more adequate minimum national standards and that the Department of Transport and Regional Services require that there is a more comprehensive training programme for all security-related airport staff.

XIII. It is recommended that the Department of Transport and Regional Services prepare regulations so that airports ensure that all those entitled to enter airside secure areas at CTFR airports in connection with work responsibilities should be subject to screening each time they enter, and potentially subject each time they leave, the secure area.

XIV. It is recommended that the Australian Government require that the screening of cargo be expanded and include mandatory screening of all cargo on passenger aircraft where passengers' checked baggage is screened.

XV. It is recommended that the Office of Transport Security in the Department of Transport and Regional Services offer appropriate and increased security-oriented training and guidance and be in communication with airports, and especially regional and smaller airports, to survey and help discern their security needs. This role should include ensuring that ASIO T4 assistance with the design of physical security infrastructure is available where necessary or appropriate, with costs subsidised by the Commonwealth.

XVI. It is recommended that a sufficiently resourced Commonwealth body, such as an enhanced role for the Science, Engineering and Technology Unit within the Department of the Prime Minister and Cabinet, be empowered to evaluate emerging technologies relevant to screening and other security-related efforts at airports and to recommend, oversee and assist the uptake of such technologies.

XVII. It is recommended that the arrangements for State or Territory Police to take over from airport AFPPS CTFR personnel in the event of a terrorist incident, along with arrangements for potential broader Commonwealth involvement, be reviewed and simplified by a senior Commonwealth/State working group under the supervision of the Secretaries' Committee on National Security. The changes should incorporate the role of the Airport Police Commander and ensure clear and consistent lines of responsibility, command, and control. The use of a command structure similar to the United Kingdom's 'Gold, Silver and Bronze' system should be adopted and include relevant industry and other non-government participants. Regular resilience exercises based on the new arrangements, which must be inclusive of all participants, should be held.

1. Introduction

1. A review of security and policing at Australia's airports by the Rt Hon Sir John Wheeler was announced on 7 June 2005 by the Australian Government, through a joint media release and media conference by the Deputy Prime Minister and Minister for Transport and Regional Services, the Attorney-General, and the Minister for Justice and Customs. Ministers noted that Sir John had established the United Kingdom's National Criminal Intelligence Service and had conducted a major review of security at UK airports including Heathrow. Sir John was to be supported by Mr John Abbott, Mr Neil Fergus, and a Secretariat.

2. The Airport Security and Policing Review was requested to report to the Government in early September 2005. On 4 August, the Prime Minister wrote to Premiers proposing a special meeting of the Council of Australian Governments (COAG) in late September dedicated to consideration of counter-terrorism issues, noting that the timing of the meeting 'will allow us to benefit from a report from the Rt Hon Sir John Wheeler on aviation security and policing arrangements at Australian airports'. That COAG meeting would, of course, also discuss lessons arising from the terrorist bombings in London on 7 July 2005 and other counter-terrorism matters.

3. The context for the review of security and policing at Australia's airports was community concern about reported instances of criminality and security weaknesses at major airports such as Kingsford Smith in Sydney. The media had highlighted the possibility that weaknesses exploited by criminals could also be utilised by terrorists.

4. The major contributors to the community concern included the Schapelle Corby case, involving a large amount of cannabis discovered in Ms Corby's luggage on her arrival in Bali after travelling from Brisbane via Sydney on 8 October 2004. The Corby defence team suggested that the drugs may have been inserted by baggage handlers or others in Australia for distribution within Australia but not recovered. On 6 April 2005, a QANTAS employee at Sydney Airport inappropriately removed a costume camel's head from a passenger's checked baggage and wore it on a tug on the tarmac. QANTAS staff at Sydney Airport were also among those implicated in an investigation involving the importation of cocaine by an organised crime syndicate.

5. On 31 May and 1 June 2005, *The Australian* newspaper ran front page and supporting stories based on a report by a staff member of the Australian Customs Service which was classified 'Highly Protected' and released without authorisation and included details of security and criminality vulnerabilities at Sydney Airport involving baggage handlers and other staff such as security screeners. The media reporting also cited theft from passengers and allegations of on-airport employee links with drug smuggling and organised crime.

6. Then Deputy Prime Minister, the Hon John Anderson, was explicit about the Government's responsiveness to the community concern at the joint media conference on 7 June 2005. He stated that "we're conscious that the community now understandably wants the issue of criminality addressed because they think that where there's a potential for terrorism ... they want any overlap addressed. ... I think it is right that governments respond to community concern. ... We want a quality overview. I think public confidence is obviously very important".

7. The Review's Terms of Reference (see p vii) were appropriately very broad, but there were inevitably limits to what could be examined in the course of three months. In relation to the first Term of Reference on the threat from serious and organised crime at airports and related cargo areas, the Review focused on Australia's major CTFR airports and on the intelligence reports it was given, as well as on submissions and visits. In relation to the third Term of Reference on the adequacy of current ground-based security requirements and arrangements put in place in response to threats of terrorism, the Review also considered non-CTFR airports and the overall legislative, regulatory and risk assessment framework. All referenced sub-points were considered, with particular attention to the ASIC card and associated background checking and access arrangements, and policing and security coordination at major airports.

8. In relation to the second and fourth Terms of Reference inviting recommendations, the Review sought to make necessary broad recommendations. It noted the important context of the need to strengthen the integration of ground-based aviation security and law enforcement arrangements. The Review also agreed that this should include enhanced threat and risk assessments and response strategies that were not only whole-of-government at the Commonwealth level but embraced the States, Territories and key private sector participants such as the airports and airlines.

9. The Review did not seek more time or resources because of the need for timely consideration of the recommendations from its overview. It believes that details of implementation, including legislative change, should be sorted out in a collaborative manner by relevant Commonwealth, State, Territory and private sector bodies.

10. The Review sought submissions through print media advertisements on 17 and 18 June 2005 and through letters directed to relevant key bodies. Major airports and some regional airports were visited around Australia, and meetings with State and Territory Ministers, Police Commissioners, industry participants and organisations were held in addition to discussions with relevant Commonwealth agencies. Sir John also met with the Prime Minister and key Ministers, with the Leader of the Opposition and key shadow ministers, with the ACTU and associated unions, and with members of the Joint Parliamentary Committee on Public Accounts and Audit. A number of classified documents were supplied to the Review, including by the Australian Customs Service, the Australian Federal Police, the Australian Crime Commission, the Australian Security Intelligence Organisation and the Office of National Assessments. These informed the Review but cannot be made public. The Review team is grateful for the access and assistance provided across Australia (Annex 1).

11. The Review was impressed by many of the measures taken in Australia since September 2001 (Annexes 2 & 3) and heartened by the additional actions proposed and agreed by the Australian Government during the Review's course from 7 June. Naturally, the Review's focus was on what could be done better, especially with respect to improving policing at airports and reducing vulnerabilities to criminality and breaches of security that might also be able to be exploited by terrorists.

12. In the course of the Review, a number of issues arose that were more appropriately dealt with in correspondence than in the final report. Sir John wrote letters to relevant Government Ministers in relation to: a potentially urgent security situation at a particular location; a nationally consistent telephone number to report security issues; the desirability of a national training and assurance regime for senior police; and revisions to regulations in relation to some prohibited carry-on and on-board aircraft items in light of the introduction of hardened cockpit doors.

2. The Importance of Airports

1. Aviation and issues surrounding it have a place conspicuously more prominent in Australia than is the case in smaller countries or in those whose closest cultural and economic ties are with their nearest neighbours. Because of the size of the Australian continent, because the major cities and towns are so far from each other, and because of the distances to the overseas destinations many citizens have in mind, aviation is disproportionately significant in Australia. With Australians exceptionally focused on aviation, government decision-makers have to treat aviation matters and issues of perception and concern with exceptional care and attention.

2. Airports are the primary hubs in our aviation system. Through them pass large numbers of passengers: each day, well over 100,000 people fly from one Australian airport to another, and almost 50,000 more leave or enter the country by air. This amounts to 100 million annual passenger arrivals and departures, of whom international passengers comprise 20 million. In addition, airports serve as freight terminals for a large and growing amount of cargo: the value of Australia's international air freight is $70 billion a year, some 8 per cent of GDP and a figure higher than the GDP of two-thirds of the countries in the world.

3. Airports are much more than just transportation nodes. They are critical infrastructure and work sites. Perhaps 150,000 people in total are directly employed in connection with the major airports in Australia's capital cities alone. Airports are retail outlets: Sydney Airport's duty free outlets, for example, sell almost 25,000 bottles of liquor and some 10,000 bottles of fragrances each week. And airports are major contributors to the local, regional, and the national economy.

4. Perhaps as important as their contributions to transportation and the wider economy is the symbolic significance attached to airports. They embody the modern world in all of its complexity, since few other places bring together our most advanced technological creations and the intricate interconnected systems we have devised to serve both those creations and ourselves.

5. Because airports attract such crowds of people, because of the high value of goods available at and filtering through airports, and because they are such conspicuous symbols of our technologies and societies, airports are obvious targets both for those who wish to attack us and for those bent on illegal personal gain. Australians would be shocked if an attack were to be made at a major Australian airport or on an aircraft that had just departed from one, but we could not be surprised.

6. It is important to note that Australia's airports present a truly wide diversity of targets. The major airports in the major cities are obviously of interest to criminals and terrorists; the concentration of wealth, people, and valuable assets, and their iconic standing, make them so. Even a small airport can support the transit of illicit goods and people, or serve as the base from which attacks on other targets might take place. And we could barely begin to count the cost, say, of an attack on a mid-sized airport near a resort, something along the lines of the recent tragedy at Sharm El Sheikh in Egypt: the damage and killing at the site at the time would be bad enough, but the flow-on costs to the aviation industry and to Australia's tourism industry, exacted over years, would be many, many times that original setback, and the blow to public confidence would be immense.

3. The Threat

1. Terrorism, organised crime and opportunistic crime constitute the major security threats to Australia's airports. The changing characteristics of transnational terrorism are well recognised in Australia and overseas (Annexes 4 and 10).

2. Substantial concentrations of goods, wealth, property, and people attract crime. Airports are no exception. The incidence of property crime actually reported in airports is low and comparable with similar areas such as large shopping centres. But, as compellingly stated in the NSW Police submission to the Review (Annex 6), criminality and associated vulnerabilities at airports make a shopping centre analogy totally inadequate. The existence of serious and organised crime, and of volume or opportunistic crime, both through and within airports, not only presents a problem in itself but also has potentially serious security implications.

3. The attributes of speed and convenience that make transport by air attractive to legal shippers of high-value/low-volume cargoes also draw the attention of those wanting to convey illegal goods, most notably narcotics. And people smugglers and those travelling illegally appear to believe that they can with some impunity avail themselves of air travel, trusting that illegals can submerge themselves in the waves of ordinary passengers.

4. That transfer of illegal goods or people through airports is neither easy nor straightforward. Indeed, that transfer would be much more difficult if not for the complicity, where it exists, of officials, aircrew, and employees working at airports. People can be tempted to turn a blind eye to illegal activity, or even participate directly in it, for a variety of reasons: financial gain, personal connections with professional criminals, even coercion. Regardless of motivation, the result is the fostering of an environment where such illegal activities as drug-running, money-laundering, and people-smuggling can be established and grow.

5. Other crime also exists at airports, involving vandalism, theft of property and mail, and even violence against people (the latter often brought about by the unfortunate mixture of alcohol, personal crises, tension connected with flying, and disappointment with flight or security arrangements). Again, efforts to halt, interdict, or even understand the incidence of crimes of this type can come up against problems within

existing security arrangements: retail outlets can just write off disappearances rather than follow up on what to them are losses to theft which are only trifling compared with sales; staff members have been known to be reluctant to report suspicious actions, even criminal misbehaviour, by their workmates; and airport authorities are likely to be in no hurry to depict the areas for which they are responsible as being rife with problems. The lack of an appropriate policing presence of airports is a major disincentive to the reporting of crime and hence to a proper appreciation of its nature and extent. The Review also found very poor data on, and little concern with, aviation cargo losses.

6. The result can be a self-reinforcing cycle. Crime can be embedded at airports. Those meant to be erecting barriers and enforcing laws against crime will not be prosecuting their jobs with full effectiveness. Criminals can become aware of where and who the weak links are, and so be able to work through or around them. The security forces can grow content with compromise, presiding over a weakened system that evokes no serious complaints, either because things have always been this way or because nothing seen as serious harm is being done. And so the cycle continues.

7. Terrorism presents a much sharper danger than does crime, because the immediate impact can be so high. The vulnerability and attractiveness of airliners and airports as targets for terrorists has been clear for decades. And it did not take the 11 September 2001 attacks in the United States to demonstrate terrorists' willingness to do harm via the air-transport systems or terrorists' inventiveness in seeking new ways to do that harm. Skyjacking, once a largely criminal or political domain, became a favoured method of terrorists by the late-1960s, sometimes resulting in the destruction of aircraft and the deaths of passengers. Since 1968, terrorists have attacked airports on a number of occasions including Athens, Lod, Zurich, Nicosia, Rome and Davao. In 1988, 270 people were murdered when a terrorist bomb exploded aboard a jumbo jet over Lockerbie in Scotland. In 1995 terrorists planned to detonate explosives almost simultaneously on eleven international aircraft, most departing from South East Asia.

8. Nor have aviation-minded terrorists rested on their laurels since September 11. Rather they have continued to demonstrate their determination and inventiveness (Annex 4). December 2001 witnessed an attempt to down a trans-Atlantic flight using a

shoe bomb. Firing shoulder-launched surface-to-air missiles, al Qa'ida operatives just missed a targeted passenger aircraft in Kenya in November 2002. Suicide bombers blew two Russian airliners out of the sky in August 2004.

9. Such terrorist actions against the aviation industry have elicited strong counter-measures by authorities, it is true. But those past actions have also demonstrated to terrorists and would-be terrorists that they have at hand a highly effective way of making a statement about their devotion to their cause, and also a way of undermining the belief of populations at risk in the ability of their governments to protect them.

10. Terrorism and crime do run together, as demonstrated to the Review by classified material from ASIO and ONA. Clearly, relations between terrorists and professional criminals will always be uneasy. The two groups are recruited from different milieux, and neither is well disposed toward outsiders. Trust can never be assured, because each side, and particularly the terrorists, will remain aware of the possibility of betrayal to the authorities. The strategic goals of the two sides are not congruent: terrorists seek the demise of the existing social order, while professional criminals are generally conservative, wanting the preservation of a *status quo* in whose interstices and problem areas they can parasitically thrive. And criminals might even come to see terrorists muscling in on their territory, since some terrorist groups have turned to crime to support themselves and their operations; the 2004 Provisional IRA (PIRA) 24 million pound bank robbery in Belfast being the most prominent recent example.

11. Even if relations are uneasy, they can exist and even endure. Terrorists have funds and so are able to pay up-front for materials that criminals can provide: weapons, identity documents, places of refuge. Criminals stand ready to deal because such transactions pay off. And both sides are accustomed to arrangements made with few questions and then kept quiet. Indeed, criminals can be making deals with terrorists without even knowing the nature or aims of their partners.

12. Where relations between criminals and terrorists do not exist, circumstances that foster criminality still leave the door ajar for terrorist activity. Loose enforcement of security regulations, the willingness to turn a blind eye to minor violations, the reluctance of witnesses to get involved in reporting incidents, all make it easier for terrorists to gain access to or knowledge about potential targets. And awareness of which officials are corrupt or

lax can enable terrorists to blackmail or bribe their way into areas where they can exact maximum damage.

4. Existing Security Arrangements

1. To counter threats associated with terror and criminality, Australia has in place systems of security arrangements covering airports and the aviation industry more generally. These systems have international dimensions, and then extend from the highest levels of government to the aprons of 186 security regulated airports and to the aircraft that use them. The systems are inter-linked, and demand not only the attention of policy, intelligence, regulatory, law enforcement, and emergency response agencies from the government side but also a focused effort from aviation-related private enterprise. They are backed up by legislation. And they have been and are being monitored and adapted through a series of reviews, of which this Review is far from being the first, and clearly will not be the last.

2. As a signatory to international treaties and agreements, Australia has obligations to take steps to safeguard civil aviation security. The most significant of those international agreements is the 1944 *Convention on International Civil Aviation (the Chicago Convention)*, which in its original form and with its subsequent revisions lays down the basis for international aviation security requirements (see below). These international requirements have expanded in the past five years, most visibly in the areas of passenger and baggage screening and the securing of cockpit doors. Australia certainly appears to be serious about meeting these requirements, indeed is out ahead in a number of areas, and is committed to adopting new international standards if and when they are further modified. However, there are some areas where Australia would do well to embrace ICAO guidance in a more comprehensive manner.

Annex 17 Requirements and Challenges

Australia is a Contracting State to the (Chicago) Convention on International Civil Aviation and has international obligations under both the Convention and its annexes. The principal annex dealing with international aviation and airport security is Annex 17. Unless it notifies the International Civil Aviation Organization (ICAO) of a difference, Australia is committed to enact Annex 17 Standards into domestic law and to seek to observe recommended practices. ICAO will be auditing Australia's compliance with the current edition of Annex 17 from late November 2005.

The required objectives of Annex 17 include: safeguarding passengers, crew, ground personnel and the general public in matters related to unlawful interference with civil aviation; establishing an organisation to develop and implement appropriate domestic regulations, practices and procedures; and ensuring that the principles applied to international civil aviation are applied to domestic aviation to the extent practicable.

Important recommended practices include protecting aviation security information; minimising regulatory interference with civil aviation; cooperating with other countries and promoting research and development of new security equipment taking account of human factors principles; screening hold baggage, and ensuring that all persons granted access to security-restricted areas and items carried are screened at random in accordance with assessed risk. Annex 17 also recommends that 'each contracting state should require that the effectiveness of individual aviation security measures be assessed by considering their role in the overall system of performance of aviation security systems'. The Review by the Rt Hon Sir John Wheeler is clearly one tangible response by Australia to this.

Australia must establish and implement a national civil aviation security programme and specify to ICAO a responsible authority as well as an organisation capable of responding rapidly to meet any increased security threat. An appropriate authority and a national aviation security committee or similar must define and allocate tasks and coordinate activities between departments, agencies and other government organisations, and airport and aircraft operators and other relevant entities. There is also a requirement for the appropriate authority to ensure the development and implementation of training programmes to ensure the effectiveness of the national civil aviation security programme and appropriate background checks and selection procedures and training and competencies, including of screeners. The appropriate authority must ensure supporting resources and facilities for security services at each Australian airport serving international civil aviation. Surveys must identify security needs and weaknesses and remedial action must be identified and reported to ICAO. Australia is required to cooperate internationally with respect to national security programmes, training programmes, and threat information.

Each international airport must establish and implement a written airport security programme appropriate to meet the national programme; coordinate implementation of security controls; arrange for the establishment of an airport security committee; develop, resource and practice contingency plans to safeguard against unlawful interference; ensure authorised and suitably trained response personnel are readily available and that airport infrastructure properly integrates security requirements.

Australian Government

3. In the Australian Government, the Cabinet and its National Security Committee set policy on aviation security. In this, they are aided by relevant Australian Government departments and agencies which can provide advice and information on aviation and security issues, and on legal aspects connected with them.

And because Australia has a federal system, the Australian Government does not act alone: aviation security, along with other security issues, is a topic eligible for discussion and review when the Australian Government meets formally, in the **Council of Australian Governments** (COAG), with the heads of Government of the States and Territories and with a representative of local government.

4. The key Australian Government departments involved in aviation security are the Department of the Prime Minister and Cabinet, the Attorney-General's Department, and, most centrally, the Department of Transport and Regional Services. In addition, crucial policing and customs agencies report to the Minister for Justice and Customs. Others involved include the Department of Immigration and Multicultural and Indigenous Affairs and the Australian Quarantine and Inspection Service, both of which maintain a substantial presence at Australia's gateway airports, tasked with screening persons and material with no right to enter the country.

5. The **Department of the Prime Minister and Cabinet** (PM&C), through its National Security Division, provides the highest levels of government with strategic advice on aviation and broader security issues. PM&C is also responsible for ensuring that all concerned, across the broad range of official bodies, address aviation security issues as far as possible with a whole-of-government approach. That approach means agencies' acting in a cooperative and coordinated manner, rather than isolating themselves in silos where they might focus on a single task and ignore the multi-dimensional nature of the challenges being faced and of the policies being pursued to meet them.

6. In connection with this coordination mandate, PM&C takes a leading role on a number of permanent committees set up specifically with the threat from terrorism in mind. The **National Counter-Terrorism Committee**, which brings together officials and representatives from the Commonwealth and State and Territory Governments and Police forces, sets out responsibilities for protecting critical infrastructure, including airports, from terrorism. The **Australian Government Counter-Terrorism Policy Committee** oversees the development and implementation of policy across the Commonwealth Government. The **Australian Government Counter-Terrorism Committee** meets monthly to evaluate where Australia stands in the war on terrorism and to review whether the national counter-terrorism alert level is appropriate.

7. The **Attorney-General's Department** acts directly against threats to aviation security in two major ways. It helps take the lead in seeing that owners and operators of transport infrastructure share information and keep up to date on the best practice available for protecting their critical assets. And it is the responsible portfolio for two vital bodies responsible for national security, the **Australian Security Intelligence Organisation** (**ASIO**) and the **Protective Security Coordination Centre** (**PSCC**).

8. ASIO is responsible for identifying and monitoring any politically-motivated threats to Australians and Australian institutions. It also has an action mandate to help contain and disrupt these threats. And ASIO hosts the multi-agency **National Threat Assessment Centre** (**NTAC**). In the NTAC, Australia's intelligence and security bodies cooperate to evaluate security-related material as it becomes available; to make judgments about the existence and significance of dangers to Australians and to Australian interests; and to issue both broad background reports (one is prepared periodically on the aviation industry) and immediate alert notices as the dimensions of threats become clear.

9. The PSCC, like the NTAC (and the Office of Transport Security), maintains a 24-hour, 7-day-a-week watch office monitoring developments which might place Australian interests at risk. Should a danger arise or an event occur, the PSCC alerts all relevant bodies and initiates a coordinated response. PSCC has two additional major responsibilities. It maintains and updates the **National Counter-Terrorism Plan** and the **National Counter-Terrorism Handbook**, formal documents which set out the framework for understanding and handling terrorism-related issues. And it plans, supervises, and records the lessons learned from counter-terrorism exercises that test Australia's responses to simulated crisis circumstances.

10. The **Australian Customs Service** (**ACS**), the **Australian Federal Police** (**AFP**), and the **Australian Crime Commission** (**ACC**), all of which are overseen by the Minister for Justice and Customs, are additional important cogs in the machinery of government meant to shield Australia's airports and aviation industry not only from terrorism threats but also from criminals.

11. Customs has front-line officers at all of Australia's international airports. Their role there is to clear all cargo and passengers entering or leaving Australia, while also identifying and where appropriate prosecuting persons involved in the movement of

prohibited and restricted goods. They also undertake the primary immigration function on behalf of the **Department of Immigration and Multicultural and Indigenous Affairs (DIMIA)**.

12. The AFP investigates serious crimes against Commonwealth law at airports, has some focus on aviation intelligence, and maintains a network of liaison officers at the major airports. In addition, the AFP through its **Australian Federal Police Protective Service (AFPPS)** provides both the initial response in addressing terrorism issues at Australia's major airports, airport Protective Security Liaison Officers (PSLOs) and the Air Security Officers who are the sky-marshals on selected international and domestic flights.

13. The Australian Crime Commission (ACC), since its creation in 2003 as the nation's primary criminal intelligence agency, is helping to investigate serious and organised crime in the transport sector. This includes developing an intelligence-enhanced assessment of the nature and extent of organised crime at airports and in the transport sector more broadly. The ACC Board is chaired by the Commissioner of the AFP and includes State and Territory Police Commissioners and the CEOs of the Customs Service and of the Australian Securities and Investments Commission.

14. A central pillar in the Australian Government's structure for enhancing protective security at airports and in the aviation industry is the **Department of Transport and Regional Services (DOTARS)**. It is DOTARS which provides industry-linked policy advice to the Government on transport, including aviation, issues. DOTARS is also responsible for the administration of a broad range of transport-related legislation, some of which requires the exercise of a regulatory function (such as the regulation of airports under the Airports Act). DOTARS is heavily involved in consultative groups which bring together government and aviation industry participants to focus on issues, including security, of mutual concern; the most prominent of these groups is the newly established **Aviation Security Advisory Forum**. In addition, DOTARS administers programs of assistance to, among others, the aviation industry.

15. Within DOTARS, the **Office of Transport Security (OTS)** handles issues connected with maritime, surface, and aviation security. In relation to aviation security, the Office:

    - provides policy advice, including advice on relevant legislation

- works with intelligence bodies to brief industry on threats
- chairs, or represents DOTARS on the major Commonwealth committees addressing terrorism and other security issues
- works with other agencies, including AusAID and the Department of Foreign Affairs and Trade, to foster Australia's interests in regional security, including aviation and maritime security.

16. In addition, OTS regulates the protective security provided by the aviation industry in Australia through:
    - active participation in relevant international forums, and the administration of measures which come out of international agreements
    - using threat intelligence as the basis for identifying the security outcomes to be achieved by airports and airlines to mitigate sources of unlawful interference with aviation
    - working with airports and airlines to assess their risks and their mitigation measures
    - auditing the compliance of airports and airlines with required security measures
    - enforcing the appropriate security-related regulations
    - maintaining a 24-hour-a-day, seven-days-a-week Operations Centre for, amongst other things, the reporting of aviation security incidents, and
    - using intelligence assessments together with the outcomes of its compliance activity to review and where necessary modify policy and security regulation outcomes.

17. A major addition to Australia's aviation security since 11 September 2001 has been supplementation of the traditional focus on the security of departing aircraft with a risk-based focus on arriving flights and their last ports of call. The OTS is an active participant not only in multilateral forums with an interest in aviation security, such as ICAO and the Asia-Pacific Economic Cooperation meetings, but also in other international arrangements for developing the aviation security capability of Australia's regional neighbours. For example, OTS assists AusAID in the design and delivery of capacity-building projects in the Pacific and Southeast Asia, and has its own officers stationed in Jakarta, Port Moresby and Manila. Much of this new focus is on aviation security at last ports of call for flights bound for Australia.

18. Broad legislation is in place to address the wide range of criminal and/or terrorist activity which can occur in and around airports and against the aviation industry in general (Annex 3). A key recent addition to this legislation is the *Aviation Transport Security Act 2004*, backed by the *Aviation Transport Security Regulations 2005*. These establish the legal framework for a security regime under which aviation industry participants themselves are required to act to reduce security risks to their operations.

State and Territory Governments

19. In Australia's federal system, the States and Territories play a vital role in aviation and airport security. It is they that have the resources and the responsibility to respond to a terrorist situation anywhere within their jurisdictions, and it is they that, for the most part, detect and prosecute criminals who operate at airports and in the aviation industry. So States and Territories must be involved both in planning and in activity at every level.

20. The Premiers and Chief Ministers of the States and Territories sit on the Council of Australian Governments (COAG); they contribute there to deliberations on all issues of security, including aviation and airport security. The National Counter Terrorism Committee (NCTC) determines and then sets out the methods all will use to try to prevent a terrorist attack and to respond should such an attack occur. In that Committee, each State and Territory is represented both by an official from the Chief Minister's or the Premier's Department and by a high-ranking officer from its Police Service.

21. The level of cooperation and coordination among Commonwealth and States and Territories established in COAG and in the NCTC is sustained in other bodies that concern themselves with security issues and with the need to address potential crises. These bodies include the Standing Committee of Attorneys-General, the Australasian Police Ministers' Council, and the Australian Health Ministers' Conference. In dealing specifically with transport security issues, including aviation-related matters, the Australian Transport Council and its Transport Security Working Group coordinate efforts.

22. Within State or Territory Governments, arrangements exist for preventing or handling crisis situations, and those arrangements largely parallel those in the Australian Government:

    - similar to the National Security Committee of Cabinet, a committee of senior State or Territory Ministers whose

portfolios encompass security-linked issues, chaired by the Premier or Chief Minister, determines strategy, sets policy, and oversees its implementation

- similar to the Secretaries' Committee on National Security, a committee of senior public servants with security responsibilities provides advice to the Ministers' committee
- other bodies and committees bring together appropriate officials and others with expertise to adopt measures to head off, to sustain capabilities for handling, and to respond to crises in particular fields or areas (eg hazardous material, explosive devices, critical infrastructure protection, postal security)
- legislation, regulations, and formal plans are in place to enable authorities to take proper measures to handle crisis situations should they develop, including measures to activate and convene a State Crisis Centre, similar to a National Crisis Centre, should the need arise to centralise information and support decision-makers.

23. In the event of a terrorism-inspired or other major catastrophic event at an airport, State or Territory Police would be called upon to respond. They in turn would be backed up by State or Territory Emergency Services, ambulances, and medical support facilities. And ultimately State or Territory engineering services, public works agencies, and welfare agencies could be factored in when the emergency had passed. Plans are in place for all of this to happen, and for it to happen in coordination with Australian Government capabilities should that prove necessary.

States, Crises, Aviation, and Airports

An example of the responsibilities, planning, and activity of States in connection with airports, the aviation industry, and the need to protect them is the way in which the State of Victoria is proceeding. The following are some of the methods and approaches taken by the Victorian Government and Victorian authorities.

The Victoria Police Force:

- is represented at the Melbourne (Tullamarine) Airport on the Airport Security Committee, Law Enforcement Liaison Committee, Airport Emergency Management Committee, Airport Terminal Evacuation Committee, Airport Relief and Recovery Committee, Airport Site Control Committee, Airport Media Sub-Committee, and Airport Communications Sub-Committee
- meets regularly with Federal law-enforcement agencies at that Airport
- regularly conducts risk assessments for policing and security issues at that Airport

- works with Airport authorities to facilitate security and emergency-response exercises there
- produces semi-annual strategic assessments on the threat of terrorism in Victoria, addressing in part the threat to aviation security.

The Victoria Department of Infrastructure:

- liaises with airport owners and operators and with the Commonwealth Department of Transport and Regional Services
- undertakes informal consultation with regional airports on security matters
- is moving to assist when smaller airports appear to struggle with security requirements and procedures.

In the event of a terrorist or crisis situation, the Victorian Government has

- a Security and Emergencies Committee of Cabinet (SECC), chaired by the Premier and including key ministers, to provide direction and policy, oversee results, consider what emergency powers might be needed, and co-ordinate public communication
- a Central Government Response Committee, chaired by the Secretary of the Department of Premier and Cabinet and including senior officials from departments along with the Chief Commissioner of Police and the Emergency Services Commissioner, to provide the SECC with advice and to coordinate government action
- an Airport Emergency Plan for Tullamarine that involves the Victoria Police, Metropolitan Fire Brigade, State Emergency Services, Melbourne Ambulance Service, Department of Justice, and Department of Human Services.

At airports

24. There is a major security differentiation between the minor facilities or innumerable bush-strips, many on private land, which can be and sometimes are used for basing or landing light planes, and some 186 functioning security regulated airports which, to a greater or lesser degree, host regular public transport activity. The 186 security-controlled airports, must have security measures in place, including means of ensuring that only authorised people are allowed into secure areas of the airport and a plan, the Transport Security Program, outlining the dangers to security at the airport and the means being adopted to mitigate those dangers.

25. Among the declared security-controlled airports, there are essentially three groups.

26. The 11 CTFR airports (Adelaide, Alice Springs, Brisbane, Cairns, Canberra, Coolangatta, Darwin, Hobart, Melbourne,

Perth, and Sydney) include the larger Australian airports, and all those which are operating as the major international gateways into Australia.[1] These airports have heightened security requirements: all passengers and carry-on bags must be screened before being allowed onto aircraft; and all check-in baggage on international flights must be screened.

27. Each of these 11 CTFR airports has a contingent of Australian Federal Police Protective Service (AFPPS) officers who specialise in Counter Terrorism First Response: the ability should a major untoward event occur to react to and evaluate and contain the danger; to seal off affected sections of the airport; to detain those suspected of involvement in the event; and to hand over control of the situation, as soon as that can be effected, to the State or Territory Police authority.

28. Twenty-eight other airports form a second group. These are the airports that were 'categorised' under the aviation security provisions of Part III of the *Air Navigation Act 1920* and already had airport airport security programs, but no CTFR, in place before the *Aviation Transport Security Act 2004* took effect on 10 March 2005. This reflects that this group of airports had a history of receiving RPT services using jet aircraft. Most, but not all, of the airports had passenger screening in March 2005, reflecting the pattern of jet RPT services that existed at the time.

29. The remaining 147 security-controlled airports have no additional specific requirements beyond those imposed on the group as a whole: protecting secure areas and having a Transport Security Program. So screening of either passengers or property is not compulsory at these airports.

30. The Review has focused strongly on three key elements which help underpin security at airports:

    - the Transport Security Program, a formal document which sets out not only the airport's goals for maintaining security in the face of its risks but also the responsibilities of the Airport Security Committee's constituent members to insure that advancement toward those goals is taking place

1 Alice Springs, Canberra and Hobart are the exceptions as they are equipped as international gateways but currently do not have regular scheduled international services. Horn Island has a RPT service from PNG but is not a major international gateway.

- the Airport Security Committee, which brings together representatives of bodies at airports with interests in and responsibilities for security, and
- the Aviation Security Identification Card system, which assesses suitability for, and helps to limit, access to sensitive areas at airports.

31. The **Transport Security Program** is mandated by legislation. Each airport owner/operator is to have one; to file it with DOTARS, which checks to see that the Program fulfils its purpose of aiming the airport in the direction of heightened security and that it does not conflict with other relevant Programs; and to modify and update it as changing circumstances require.

32. The **Airport Security Committee** at each airport is a formal body where representatives of government agencies and private businesses operating at the airport convene regularly to run through and discuss security issues of interest to each and all. These bodies are usually under the chairmanship of the airport management, and are intended to foster the free exchange of security-related information and the venting of security concerns. At smaller airports the Committee might consist of only a few members who are centrally involved in security matters, but at Australia's 11 major airports the Committee is likely to have representation from:
    - the owner/operator of the airport
    - the airlines that use the airport
    - air cargo agents
    - fuel and telecommunications companies
    - the Australian Federal Police which at CTFR airports is represented by AFP officers or by the Protective Security Liaison Officer (PSLO) network charged with aviation industry liaison responsibilities
    - the police force of the State or Territory in which the airport is located: this force will generally have the responsibility of performing such community-policing tasks as responding to reports of crime or of disturbances of the peace in the groundside area of the airport
    - the Australian Customs Service
    - the Australian Quarantine and Inspection Service

- the Department of Immigration and Multicultural and Indigenous Affairs
- the Australian Security Intelligence Organisation
- Airservices Australia, which provides air traffic control and airport rescue and fire-fighting services
- other organisations or businesses which have a security role or interest, and
- the Australian Federal Police Protective Service (AFPPS), which at these airports has the responibility for delivering Counter-Terrorism First Response: the ability to react quickly to identify and contain acts or threats to aviation that may be terrorism-related.

33. In addition, these 11 CTFR airports have an **Australian Government Agencies' Airport Security Committee**, which brings together the Commonwealth agencies at the airport to seek to ensure they are up-to-date and on the same page with their responsibilities.

34. For security purposes, airports can be divided into zones, the most common being landside, which is open to the public at large, and airside, which is accessible only to ticketed passengers (and others who undergo screening), to authorised government officials and law enforcement officers, to authorised airline industry personnel, and to authorised visitors or temporary employees or contractors accompanied by ASIC-holders. This division is meant to protect those assets most at risk: the tarmac, the apron, hangars and maintenance areas, cargo sheds, and the aircraft themselves.

35. An ASIC is issued to an employee with a job-related requirement for unaccompanied access to a secure area of an airport. It is issued only after successful completion of a background check which includes police and national security authorities and, in the case of non-citizens, a check of immigration status. An ASIC must be worn openly at all times when an ASIC-holder has a legitimate work-related purpose for being present in any secure area. Division 3.2 and Part 6 of the *Aviation Transport Security Regulations 2005* set out the relevant Australian legal requirements for ASICs that reflect Australian Government policy and operationalise the ICAO Annex 17 standards. For example, regulation 6.03(3) provides that an Australia-wide ASIC has effect for the purposes of entry to a secure area at any security controlled airport. There are

currently 188 ASIC issuing bodies including the 147 additional security-controlled airports with regular public transport (RPT) services that became issuing bodies this year and which are required to issue ASICs by 31 December 2005 to those who regularly need to access secure areas.

Policing

36. To link and thus reinforce the counter-terrorism capabilities of the AFP and the State and Territory Police, Joint Counter-Terrorism Teams exist in every jurisdiction. These are made up of officers from both police forces, who together investigate terrorism-related threats and potential threats, including any at or against airports. They also stand ready to serve as the nucleus for post-incident investigation should a major event occur. In addition, Melbourne, Sydney, Brisbane, and Perth airports are designated as the bases of 'Regional Rapid Deployment Teams', each in theory composed of eight AFPPS officers trained in CTFR techniques, though the Review did not find them everywhere up to strength and ready to deploy. These teams are meant to move quickly to regional airports to strengthen CTFR capability when intelligence indicates a possible threat is in store, in order to head it off or help to contain it. Their main task in the absence of threats is to conduct planned exercises at regional airports, to boost local awareness of counter-terrorism capabilities and of broader security needs. The name appears to be somewhat a misnomer because response is rarely 'rapid'. These teams should come under the command of the Airport Police Commander of the airport where they are based but continue to provide the essential support services to regional airports outlined above.

Physical security

37. Airports inevitably occupy large areas of ground. Airports in Australia, as well as elsewhere, have set up different levels and layers of physical barriers. These are tightest and most complex where the danger of penetration is deemed to be highest and where the cost of an attack would be heaviest, at the terminal and on the apron.

38. The National Critical Infrastructure Protection Program (NCIP), administered by the Australian Government Attorney-General's Department, has mandated that all security planning for critical infrastructure should be predicated on security risk assessments which must be based on and consistent with the

'Australian and New Zealand Standard for Risk Management' (AS-NZS 4360:2004)[2].

39. While this standard does not have legislative authority in Australia, it has been widely recognized by the Australian courts as being the applicable test for reasonable corporate and individual management of risks. Any failure to adhere to this standard creates a *prima facie* liability at law.

40. There are a number of other Australian standards directly relevant to the physical security of facilities, as well as in relation to emergency management planning.[3] These include the following:

    - IT Security (AS13335:2003)
    - Security Fencing (AS1725:2003)
    - Electric Security Fences (AS/NZA 3016:2002)
    - Intrusion Alarm Systems (AS2201:2004)
    - Guards and Patrols (AS4421:1996)
    - Emergency Management Planning (AS3745:2002).

41. It is axiomatic that all Australian airports comply with the relevant Australian standards when implementing or enhancing physical security measures or preparing emergency management plans. Notwithstanding the need to comply with such standards, the *Aviation Transport Security Act 2004* also prescribes requirements for airport areas and zones, including airport security zones and other security measures. The Act also requires certain aviation industry participants to have a Transport Security Program (TSP) to operate their businesses. For example, any operator of a security controlled airport or an operator of a prescribed air service is bound by this Act.

42. The *Aviation Transport Security Regulations 2005* prescribe that airport operators' TSPs must include a statement outlining the local security risk context of the airport, including a list of general threats and generic security risk events to people, assets, infrastructure and operations.

---

2 Australian standards are produced by Standards Australia International (SAI), which is affiliated with the International Standards Organization (ISO).

3 It should be noted there is also Federal and State legislation directly relating to emergency- management roles and responsibilities.

43. The Australian Government provided guidance material for security risk assessments at 'new entrant' Regional Airports in 2004. It also provided funding support for security measures. The major airports have continued to do their own security risk assessments in order to assist in the development of their TSPs.

44. With regard to perimeter fencing at airports, consideration should be given to the different needs of an isolated airport in a rural area, where the biggest danger may well be having stock or wild animals wander onto a runway, and of a heavily-used airport in an urban environment. Airport authorities are aware of the fact that perimeter fences are merely static barriers, and will need patrolling, alarm mechanisms, lighting during hours of darkness, and even security-camera coverage if they are to stand up as significant deterrents to those seeking to penetrate airports illegally. In many circumstances this is not warranted.

45. Access points through the fencing have to exist to enable deliveries of goods and equipment. Moves are already under way to reduce the number of such points, and to have personnel, vehicles, and cargoes checked before being permitted to enter through key access points at CTFR airports. Cargo, and particularly that transported on passenger aircraft, demands special treatment.

46. Historically, the greatest vulnerability has proved to be at or through terminals, and it is here that security barriers are most heavily employed. Baggage which is to be loaded aboard aircraft for international flights is already screened for explosives. Screening of checked baggage for domestic flights out of CTFR airports will be required by August 2007. Passengers, aircrew, and their carry-on possessions, before they are permitted near the aircraft, are screened through metal-detecting devices, and may be further screened through visual checking or frisk-searching. And airport employees, though they have already been approved for an ASIC and are frequently limited to entering only those areas where their work requires them to be, can also be screened, though this is not yet required under the Regulations. The Government has decided that measures will be put in place to require the screening of personnel and vehicles at the airside boundary.

47. Airports also increasingly make use of closed-circuit television camera (CCTV) coverage of vulnerable areas, both in spaces open to the public and in secured areas. And the presence of uniformed police patrolling, when and where that occurs, adds further to physical security at airports.

Aviation security reviews

48. There has been a raft of reviews connected with aviation security in Australia since the 11 September 2001 attacks in the United States, and the sequence will not end with this Review.

49. In the immediate aftermath of September 11, Mr Robert Cornall, the Secretary of the Attorney-General's Department, headed an examination of the nation's security and counter-terrorism arrangements, and important parts of that Review dealt with the aviation sector and led to further reviews during 2002 of passenger- and baggage-screening and of access control.

50. In late 2002, Mr Rex Stevenson AO presented a classified review to the Attorney-General's Department into the effectiveness of aviation security measures already adopted in Australia, including the Counter-Terrorism First Response capability at airports.

51. In January 2003, the Auditor-General presented an Australian National Audit Office (ANAO) performance audit on the response of the Department of Transport and Regional Services to the increased threat to the security of aviation since 11 September 2001.

52. In mid-2003, in response to an ASIO Threat Assessment on the dangers facing the aviation sector, the Secretaries' Committee on National Security (SCNS) initiated a further review of measures taken and measures needed to protect the sector.

53. In 2003–2004 the Joint Committee of Public Accounts and Audit (JCPAA) held an inquiry into, and in June 2004 published a Report on, aviation security.

54. In the aftermath of the Madrid bombings in 2004, Mr Ken Matthews, the then Secretary of DOTARS, led an Overseas Mission on Transport Security; he and the senior officials involved reported back to the Government on their findings.

55. Additional reviews and checks are in progress or under consideration and include the following:

    - the Joint Committee of Public Accounts and Audit has re-opened its examination of developments in aviation security
    - the US Department of Homeland Security Transport Security Administration (TSA) has been undertaking formal inspections of arrangements at Australian airports which provide last ports of call for flights to the US; while these

are not an ICAO-like audit, TSA findings will be considered by Australia's aviation security authorities

- the Secretaries' Committee on National Security (SCNS) has initiated a further inquiry in security in the aviation sector and its results are to be reported soon
- the Australasian Police Ministers' Council has commissioned research into the appropriate mix of law enforcement resources at airports, including state police resources, based on an intelligence assessment of criminal activity
- the Australian Crime Commission is pursuing work into criminality and policing at Australia's airports
- as part of its universal security audit program, the International Civil Aviation Organization (ICAO) will in late November 2005 be auditing both Australia's regulatory framework on aviation security matters and international operations at Sydney's Kingsford Smith Airport against the standards and recommended practices in Annex 17 to the Chicago Convention.

56. Partly as a result of these inquiries and reviews, and of the recommendations and actions they produced (or, like the current Review, are expected to produce), measures have already been undertaken or are being introduced to: tighten up the ASIC system for employees at airports; extend and improve the screening of passengers, luggage, and freight; strengthen security measures aboard and around aircraft; increase the number of officials with security-related responsibilities at airports and improve coordination and communication among them; boost training and exercises so that responsible personnel are better able to handle everyday security situations and potential emergencies; and strengthen the ability of the Office of Transport Security in the Department of Transport and Regional Services to audit and regulate the industry's security systems.

5. International Developments

1. In order to gain perspective on security and policing at Australia's airports, the Review undertook to consider arrangements at broadly-comparable airports overseas. Initially, consultations were held with London's Heathrow and Gatwick Airports and at Changi Airport in Singapore to enable the Review to focus on appropriate subjects for examination in Australia. Later discussions were initiated in Hong Kong, Canada, and the United States, specifically addressing the key topics of:

    - background checks for aviation-sector employees whose work would take them into secure areas at airports
    - the means and methods of limiting access to airside
    - screening of passengers and others as they enter and leave secure areas, and
    - police force arrangements at airports.

The following sections summarise the unclassified findings from these discussions.

Background checks (ICAO Standards 3.4.1 and 4.7.2)

2. All the systems used for background checking appeared to comply with International Civil Aviation Organization (ICAO) Standards and all permitted no exemption to their own rules that disqualification would occur if personal history checks and criminal history checks showed up offences in the previous ten years.

3. Some international locations had already enhanced their background-checking by using fingerprinting for identity and by further investigating credit ratings, known associations, and views of previous employers. All are working toward linking their checking systems into police networks, in order to be able to obtain early information on recent criminal offences committed by persons already on their records.

4. The importance of establishing one agency to be responsible for conducting and coordinating the background checking has been identified. So has the need to recheck backgrounds fully on a

regular basis: some do this every two years, some every five. The general judgment is that supplementary checking between those regular reviews will be unnecessary once live feeds from police records are linked into the information systems of the central background-checking agency.

5. Time taken to complete a background check varied. One authority claimed it could even accomplish the task in as little as three hours because of integrated IT databases. More standard was around a week. Difficult cases, such as those where applicants had lived overseas for extensive periods, could take much longer.

Access control (ICAO Standards 4.7.1 and 4.7.3)

6. While those at the leading edge of security consciousness and capability are clearly heading in the same direction with regard to their background checking systems for the aviation industry, there is still a wide variety of methods to control access at airports. This is caused, not least, by the wide variety of airports: newer airports had been designed with security as a top priority; older airports had not. Consequently, newer airports have remarkably few access points to secure areas and can cover them thoroughly, while older airports can have scores of access points, and if each were to be covered by a full panoply of security devices backed up by guards, the cost would be enormous.

7. It is fully recognised that access at even the weakest points should be automated and integrated: card readers must be employed; they must be backed up by such secondary measures as pin codes or biometric readers; and the process of entry should be monitored by CCTV.

8. At those airports with only few access points, and at the most important of the access points at other airports, access is more fully controlled. Walk-through metal detectors, x-ray machines, and metal-detecting wands are employed, and a guard is posted to check the ID photos on cards against the faces of those entering. Entering vehicles can also undergo thorough examination, including having their number plates recognised, their drivers screened, their cabins checked, and their undersides examined by mirrors.

9. Attempts to strengthen access control continue to advance: older airports are reducing the number of access points, and new identification methods, new machinery, and better recording systems are being trialled.

Screening (ICAO Standards 4.1, 4.3.1, 4.3.2, 3.4.2, and 3.4.3)

10. All are going in the same direction with the screening of passengers, their carry-on possessions, and their check-in baggage:

    - modern equipment is employed in the form of walk-through metal detectors for passengers, x-ray machinery for possessions, and explosive detection devices; these are supplemented where necessary by trained personnel who will search belongings and pat down passengers, including in private screening facilities
    - screeners are uniformed, trained, and certified; screeners are frequently tested, and undergo recurrent training, and
    - all screening points are covered by CCTV.

11. There is diversity in identifying people who are not subject to screening. For instance, in one place only Heads of State and uniformed police are not screened. In others, the list can be substantially longer, and even include airport workers.

Policing (ICAO Standards 3.1.8 and 3.2.5)

12. Again, a single pattern emerges: major airports are treated as separate local police commands, and it appears that a strength in the order of 400 officers is not unusual (Annex 7). These officers are posted from the local police force, do all policing in and around the terminal and the other areas of the airport, have the power to search and have trained dogs and equipment available to assist in this, and include officers trained in specialist airport counter-terrorism methods.

13. Police Commanders at these major airports overseas are responsible for all the policing functions there, and they both maintain direct lines to the airport authorities and report through normal police channels. In all cases, contingency plans exist to back-up airport police with response teams and with the Defence Force in the event of a major terrorism incident.

6. Weaknesses in the Present System

1. Despite the substantial efforts and resources put into aviation and policing-related protective security in Australia, weaknesses remain. Some are minor and easily addressed or do not carry risks justifying additional measures. Others are substantial, even systemic, and will call for determined action if things are to be put as right as they can be. While it is true that there is no such thing as 100 per cent security, at airports or anywhere else, that is no excuse for putting off the changes needed to improve the situation.

Cultural issues

2. Security and policing at Australian airports, like other human endeavours, display characteristics that can be described as their 'culture'.

3. The Review encountered three particularly striking elements of the airport security and policing culture at most major airports:

   - a marked inhibition about sharing information with those who need it to make evidence-based decisions
   - a lack of clarity, consistency and alignment between authority and responsibility in decision-making, and
   - an undue reliance on 'after the event' compliance auditing, rather than 'pre-event planning' as the basis for accountability.

4. These are critical issues that need to be addressed. It is suggested that the Airport Security and Policing culture needs to move to a position:

   - where agencies which have a responsibility to collect information relevant to the threats and risks encountered in providing airport security and policing also have the complementary knowledge, attitudes, skills and procedures for facilitating the sharing of that information with those who have the responsibility for making decisions about airport security and policing
   - where there is alignment so that those who own the risks also have the responsibility for providing (and funding) security and policing and the authority (including control

over deploying resources) to provide those services, and those who have responsibility and authority are accountable; and

- where the monitoring of compliance with security and policing plans makes an important contribution to the sources of information in the planning process rather than being seen as the predominant source of accountability in airport security and policing: compliance auditing is a contributor to good security and safety planning, not a surrogate for it.

Information sharing

5. Private sector elements are crying out to be brought up-to-date and kept up-to-date on the dangers they face from crime and terrorism. But while there have been improvements, many public and private sector organisations have their own files and their own data on crime or criminal-related activity, and cite either privacy legislation or their need to protect themselves from their competitors as reasons why they cannot share this information. Without the contribution of their knowledge, the job of gathering information can never be more than half done.

6. Both in capitals and in airports, different government agencies still struggle to break their long traditions, perhaps developed at a time when intelligence had a different function in a different struggle for security and the rule of law, of keeping their knowledge to themselves. Good reasons are advanced for this: fear of leaks that might endanger covert sources or methods; the need for police to protect operational information which ultimately has to be used for successful prosecutions; the concern of Customs officials not to trample on legislation and not to risk exposing their own operational methods; and so on. Good reasons. But not good enough for the culture required to cope with contemporary challenges.

7. Until all connected with aviation and airport security put into practice the idea that information is a primary weapon in planning the protection of the Australian community from crime and terrorism, and that sharing information is a means of sharpening that weapon, the security system will falter. The way in which institutions set themselves up as silos and keep their security data and ideas to themselves must end. Clearly this involves strong leadership, direction, and enforcement from the top of all institutions. If it also means legislative review and change (and it will), let that be done.

Aligning responsibility and authority

8. The framework for Australian airport and aviation security, as it is set out in legislation and brought up frequently at meetings by officials and businessmen, is that both the ownership of the risk posed by terrorism and crime and the responsibility for security are shared between government agencies and private sector participants in the industry. An unambiguous understanding of, and positive attitude toward, this sharing was seldom, if ever, as evident in practice as it was prominent in theory.

9. There was all too frequently a perception that government decisions imposing additional security-related obligations on industry are taken without the serious consultation that effective partnership and sharing entail. Review members faced business interests readily acknowledging that 'providing security is part of the cost of doing business,' while almost simultaneously, complaining that government was failing to absorb more and more of that cost. There were repeated arguments against the need to demonstrate leadership in dealing with risks to their own enterprise as industry representatives waited to be directed to take action by legislation or other government regulation, appearing to imply that the duty of care to their staff and passengers was not much of an issue.

10. Cost issues connected to security appear to be the most vexatious, and the behavior of the public sector has not always helped: in allocating some of the funds for screening equipment and for cockpit doors, for instance, government seemed to be guided by the principle of 'capacity to pay' rather than by any clear idea of how responsibility for security and ownership of risk were to be shared. 'Capacity to pay' can be a reasonable basis for policy, but it is not the same as 'security is part of the cost of doing business'. Protracted and seemingly irreconcilable debates about who should pay certain costs can be expected to continue in the absence of an agreed and documented statement of the policy principles for allocating costs among the Australian Government, State/Territory Governments, and private sector owners/operators.

11. In the midst of this complexity, it is no surprise that public agencies, private operators, the media and the public appear to lack clarity about who is to be held accountable for which aspects of airport security and policing.

Compliance auditing

12. The concept and practice of governments establishing legislated minimum standards for security measures to be implemented by airports and airlines is central to the international approach to airport and aviation security that is coordinated by the International Civil Aviation Organization (ICAO). Furthermore, the performance of government agencies throughout Australia is subject to auditing by respective Auditors-General. The Review was presented with no evidence questioning this approach to either government administration in general, or airport security and policing in particular: the Review supports the continuing importance of auditing of this nature. 13. On the other hand, the Review did find some evidence suggesting that there may be grounds for rethinking the role that compliance auditing is perceived to play in airport security and policing.

14. For example, reference already has been made to a repeated comment from some industry representatives along the lines that it was their respective responsibility to do what was required of them by government regulations administered by the OTS. In their view, the more detailed and prescriptive the regulations the better, as this would help with boards and insurers. In contrast, more sophisticated industry members such as QANTAS argued for a principles and risk-based approach tailoring the applied measures to assessed risks. The Review would prefer to see a culture in which each organisation took responsibility for demonstrating leadership in assessing threat and risk on an ongoing basis and fulfilling its responsibilities for the safety and security of its staff and customers.

15. ANAO performance audits of aviation security in 1998 and 2003 have focused attention on the compliance auditing function of what is now the OTS within DOTARS. The 2003 Report (No 26, *Aviation Security in Australia*) devotes two chapters to compliance and concludes that DOTARS should "properly hold airports and airlines accountable for their actions and, in turn, aim to ensure that airports and airlines hold their contractors who breach the security requirements to account for their breaches".

16. Furthermore, Australian media are replete with stories about 'aviation security incidents' suggesting that identification of a 'security breach' or a breach of the law at an airport represents a 'failure' of security or law enforcement. Law enforcement, including the enforcement of security regulations, is an

important component of the struggle against criminality and terrorism, but no law or regulation – and no amount of compliance auditing – can force compliant behaviour in all circumstances. It is not practical or of priority in many circumstances to prevent breaches of airport boundary fences when the focus should be on the aircraft on the apron and the security of the terminal and air traffic control. Counting the number of occasions on which non-compliant behaviour is detected is not necessarily the most useful way of measuring the effectiveness of Australia's airport security and policing system. It is more important to measure the effectiveness of the system in mitigating the threats and risks it has been established to counter.

17. Monitoring and auditing compliance with security measures is an important component of any airport security and policing regime, particularly as a source of information for security and policing operations planners. However, it is not the sole determinant of the effectiveness of that regime, and it is more important to give priority to building a robust system than to increasing the prominence and resources devoted to monitoring compliance with a potentially sub-optimal security system.

18. The likely amendments to Annex 17 to the Chicago Convention will increase the focus on risk assessment at individual airports. The current version of ICAO Annex 17 includes the recommendation (paragraph 2.2) that each Contracting State should whenever possible arrange for the security controls and procedures to cause a minimum of interference with, or delay to the activities of, civil aviation provided the effectiveness of these controls and procedures is not compromised. This suggests an emphasis on simplicity and cost effectiveness rather than just regulatory compliance. To achieve the desired balance between audit and facilitation of an appropriate risk-driven industry methodology, it will be necessary for the Office of Transport Security to foster the right culture among its own staff.

Intelligence

19. The first line of defence against criminals and terrorists is an informed understanding of their intentions and capabilities. This is as true at airports as it is elsewhere. Informed understanding of those who operate in the dark, as terrorists and criminals do, rests mainly on intelligence: the widespread, sometimes-clandestine gathering of information about them, followed by careful, centralised analysis of this incoming

information, done against the background of previous conclusions about them and of comparisons with similar actors in other places.

20. In Australia, this process against potential terrorists results in national security Threat Assessments, formal reports issued by the Australian Security Intelligence Organisation (ASIO). Seeking to understand the causes of terrorism and to combat the promulgation of strains of religious extremism and aberrant ideology, especially among young people, that lead to terrorist acts is a major priority for security services in Australia and internationally. However, the Review was unable to ascertain the success of ASIO's understanding of these groups in Australia. With regard to airports and the aviation industry, ASIO can issue an immediate Threat Assessment making judgments about the danger to a particular target at a particular place at a particular time. ASIO also puts out a more general Threat Assessment evaluating the known and likely dangers posed by terrorists to the aviation industry as a whole. Others, then, with a security interest in the industry can use these Threat Assessments (if necessary via the OTS) to make their own judgments about the terrorist risks they and their assets face, and about what they must do to mitigate those risks. ASIO has also established a network of 'liaison' officers at major airports. However, typically this liaison is viewed as one-way. Sharing of aviation-specific information and intelligence assessments by ASIO with appropriately cleared members of the State and Territory Police, and the wider public and private sectors within the aviation industry should be further improved, and aviation and airport-specific assessment material produced and distributed more frequently.

21. The Australian Crime Commission (ACC) collects data on crime and produces annually a snapshot of general criminality in the country as a whole. The ACC is also moving to institutionalise production of National Criminal Threat Assessments looking at criminal groups, their intentions and capabilities, and the crimes in which they specialise. But nothing resembling the ASIO terrorism-oriented process for the aviation sector exists for criminality at airports. Information-gathering about the methods and plans of criminals at airports is sporadic. And there is little in the way of centralised ongoing collection, collation, and rigorous analysis of such information. Consequently, there is no such thing as a variant of a Threat Assessment addressing criminality either at a particular airport or more generally in the aviation sector. And this largely leaves

the victims and potential victims of crime in the industry to try, on their own or in conjunction with colleagues and local law-enforcement officers, to understand what has affected them in the past and do their best to cut back on such attacks in the future.

22. The Department of Transport and Regional Service, through OTS, has distributed, and various police forces have been putting out, reports on the national security risks the aviation industry faces. But many at airports, and at the smaller airports in particular, feel that they are left out of the loop when it comes to intelligence about security concerns (see below). They sense that information, including classified information, on the security and criminal threats their industry faces is being collected and processed. But they believe that their need to keep up with developments is being underestimated, and that the common observation that any chain is only as weak as its weakest link seems to be forgotten where they are concerned.

Airport policing and security at regional airports

The position of the Police Superintendent at a regional centre like Dubbo with its own airport illustrates the dilemmas of many outside the major cities. Police and the local airport authorities are on fine terms, and judge themselves well prepared for a crisis:

- they have an easily-understood emergency plan in place
- those likely to be involved know the step-by-step procedures
- each police car carries a copy of the plan.

But he and his forces do not believe that they are plugged into the bigger picture:

- they receive no regular bulletins or information on threats to aviation or how to counter them
- information on counter-terrorism issues is sporadic and unfocused
- they had been led to believe that assistance would be provided to have CCTV in operation at the airport fed to the Police station; this has not happened
- aware of the danger that unscreened passengers from the local airport could create in Sydney after arriving there, he believes his forces could help, but he needs guidance on what kind of information his forces should be gathering, how to gather it covertly, and how to process, analyse, and report it.

The Review was impressed by the arrangements it saw at Dubbo. However, the realistic desire for more information was common among larger regional airports and their police management.

Chain of command

23. Among the systemic problems identified at major airports is the issue of law enforcement command and control. Bluntly put, in the everyday workings of airports, no one is taking overall charge of policing and security. Many capable institutions, agencies, and people play a part, and they can and do cooperate with each other and attempt to coordinate their actions. But much of what each does is done in isolation, and much of what they do in conjunction or together is done because of good intentions, good will, and good personal relations. Such stuff is admirable. But it is too ephemeral and inconsistent to serve as the solid foundation of a security and policing system where reliability and responsibility are permanent features.

24. It is a cause for concern that response arrangements for potential significant incidents or crises at major airports, where lives have been taken or could be at risk, lack lines of authority of adequate clarity, certainty and efficiency. It is not always clear who is in charge and in which circumstances, how that responsibility is to be transferred from one body to another, and how those bodies are to communicate in a crisis.

25. One glaring example is the failure to provide effective arrangements to enable AFP, AFPPS and State and Territory Police services to communicate with each other, and with other airport security personnel, especially in time of emergency, when perhaps mobile phone communication is unavailable. The Review was told about this deficiency at a number of major airports.

26. The Australian Federal Police Protective Service contingent at major airports, with its Counter-Terrorism First Response role, is meant to contain the crisis until the State or Territory Police arrive. But exactly when that time might be is not clear.

27. Some of these command-and-control problems have their roots in the splitting of policing functions at Australia's major airports and in the related gaps in acceptance of responsibility and deployment of resources. At these 11 major airports, CTFR is the task of that special contingent of AFPPS officers. But the task of so-called 'community policing' at airports, which involves handling disturbances of the peace and investigating crimes, remains the responsibility of the local State or Territory police. And at almost all major airports those police have no established post, or even a permanent presence: Melbourne Airport alone has a permanent presence, of two police officers

who work during normal business hours (Annex 7). The roots of this lack of on-airport community policing are based on historical Commonwealth/State issues (see below).

An overview of airport policing in Australia

Available records suggest one of the reasons for the inadequacy of policing at major Australian airports is confusion and unresolved funding issues between the Commonwealth and the States and Territories. The key chronology is as follows.

Commonwealth Police (plainclothes) policed airports in Sydney and Melbourne in the 1960s and other major airports as they opened. An 'enhanced airport security' decision in December 1974 incorporated an additional 333 uniformed Commonwealth Police, specially trained and more highly paid, to be stationed at major airports.

The *Commonwealth Places (Application of Laws) Act 1970* and relevant gazettals provided that State police duties under State law also apply at Commonwealth 'places' such as airports (Section 52(i) of the Constitution refers) and if State Police observe a crime at an airport they have a responsibility (sworn duty) to take appropriate action.

The Australian Federal Police (AFP) was established in 1979 and replaced the Commonwealth Police. Section 8(2) of the *Australian Federal Police Act 1979* provides that the provision of police services at Commonwealth places such as airports in relation to State offences 'shall be in accordance with arrangements made' between the AFP Commissioner and State Commissioner. The AFP advises that no such arrangements have been made. AFP officers have the necessary powers to enforce State laws in Commonwealth places under Section 9 of the AFP Act.

The Australian Protective Service (APS) was established from October 1984. In 1986 a review of Australia's counter-terrorism capability highlighted inadequate airport protection and recommended the formation of a specially trained Commonwealth airport police force.

In May 1989, Prime Minister Hawke wrote to Premiers seeking to transfer the AFP uniformed community policing function at airports to the States and NT together with the counter-terrorism first response (CTFR) role to ensure a single police force at each airport. While Premiers' agreement on the transfer with accompanying relevant funding arrangements was sought, this was not achieved and an impasse emerged.

In November 1989, the Hawke Government decided to transfer the CTFR role from the AFP to the APS by June 1990. In 1991, as a result of international terrorist threats, APS airport staffing was raised from 300 to 370. In the absence of regular State or AFP policing at airports, APS officers had a significant *de facto* community-policing role which continues today. The APS became an operating division of the AFP from 2002 and was fully integrated on 1 July 2004.

State police forces have provided some community policing at airports, depending on special events and their other resource priorities. For example, NSW Police had an integrated presence with the AFP and APS at Sydney Kingsford Smith Airport during the Olympics; and Victorian Police had a significant community-policing presence at the Melbourne airport (Tullamarine) until 1999, when other priorities intervened. State police from local area commands continue to respond to airport incidents of crime on a priority basis.

27. This division of policing responsibilities has three important drawbacks:

- First, it can mean that neither task is performed as well as it might be. Pressure is put on the AFPPS, who are already on the scene, to handle community policing problems when those develop quickly, and this can distract the AFPPS from CTFR responsibilities. Meanwhile, State and Territory Police, judging that comparatively little crime occurs at airports and that some uniformed presence is already there in the form of the AFPPS, can assign less in the way of community policing resources to airports than is actually needed.
- Second, a disconnect can occur between the information-gathering and information-sharing of the AFPPS and State and Territory police. Because of the closed nature of collecting and analysing intelligence-related material, full cooperation in this field between the two services is unlikely. But criminals and terrorists, as they plan, prepare for, and follow up on their operations at airports, easily straddle the gap between the separate knowledge bases of the two police forces and also of the Australian Customs Service.
- Third, and most worrying, the division of responsibilities can create uncertainty and confusion over authority at crucial times. In the event of a serious crime, for instance, an AFPPS officer, with only limited powers of arrest and detention, may have to intervene initially, then hand over a suspect to the State Police when they arrive, and finally serve in the capacity of private citizen as a witness at a State court. In the event of a terrorism-related crisis, the uncertainty over when and how command might pass from the AFPPS CTFR force to the local Police, and the piecemeal ways in which those police might arrive on the scene, could mean a mingling of forces, a lack of clarity among individual officers about yielding and taking over responsibilities, and a situation where control is more nominal than real.

Poor data on airport crime and criminality

28. The Review requested data from all State and Territory police forces, as well as from the AFP and the ACS, on levels of crime at airports. The Review received inconsistent data from the States and Territories, making accurate comparisons unlikely. This is in part due to inconsistent reporting methodologies. It may also be attributable to a failure to report all incidents accurately. For example, the Review noted on occasion that the AFPPS appears to treat a community crime-related incident in-house, without referring it to the State or Territory police.

29. Data received from the AFP indicates that AFPPS officers deal with a large number of security-related incidents at airports. If this is so, the Review remains concerned that those officers may still be expending a disproportionate amount of their patrol time conducting semi-policing duties to the detriment of their core CTFR and security responsibilities.

30. No one agency has the full picture on the nature and extent of criminality at airports. Customs can provide accurate data on drugs and records detections of prohibited imports and referrals to other agencies. So effectively assessing the nature and extent of other areas of criminality, such as money laundering and people trafficking, is not feasible. DIMIA maintains data on the number of people refused entry at the border. The reason for refusing entry may include criminal concerns, traveling on fraudulent documentation, or being involved in immigration related fraud such as people smuggling, and other irregular movments. The DIMIA Intelligence Analysis Section's new Border Intelligence Officer (BIO) network will become operational from early October 2005. The role of these new officers will be to enhance immigration itelligence collection and analysis at key ports Australia-wide, provide specialist intelligence support and advice on immigration issues and developments at those ports, and provide a liaison and conduit point with DIMIA's partner law enforcement and border security agencies on intelligence.

31. In sum, the Review, given the poor and incomplete nature of the data received, was not in a position to provide an accurate picture of criminality at Australian airports (Annex 5, Annex 20). The Review notes that agencies such as the AFP and the ACC are currently conducting investigations to attempt to fill intelligence and information gaps regarding crime at airports, and in the transport sector more generally. Clearly, more work must be done, including to enhance the comparability of data among State and Territory crime-reporting systems and sharing

of data, if an accurate and useful national picture of airport and aviation crime is to be developed.

Airport security arrangements

32. The Review has identified vulnerabilities in each of the three key pillars of preventative security: the Transport Security Program, the Airport Security Committee and the Aviation Security Identification Card as well as aspects of physical security arrangements.

Transport Security Programs (TSP)

33. An airport's Transport Security Program, and those of the other agencies and businesses at the airport, is a comprehensive guide to the security situation and to steps needed to improve it. But the Program, especially at major airports, can be a bulky and unwieldy document, inhibiting effective consultation and engagement with it. And a TSP has little capability for rapid adaptation, potentially leaving it slow-footed should the security environment begin to change quickly.

Airport Security Committees

34. Most Airport Security Committees provide a useful forum for exchanging ideas and bringing agencies up to date on broad security developments. But often these have large memberships, sometimes upwards of 30, and whilst they can have enthusiastic leadership, they lack real power or authority. Because membership is so wide, it cannot share information which is based on classified reporting nor can it serve for discussion of security-related operations which may be occurring at the airport or focus on ongoing threat and risk assessment.

Aviation Security Identification Card (ASIC)

35. The Australian Government has announced plans to provide a more stringent test for obtaining and continuing to hold an ASIC. These plans are sensible given that the current system for issuing and holding ASICs has many vulnerabilities including:

    - fraudulent identification may be used to enable an applicant to avoid scrutiny of his or her identity and past background
    - the background checks for applicants turn up only those who are already assessed to be national security threats or who are already on record as having served sentences for serious crimes: this assumes that historical information is an adequate predictor of future behaviour

- background checks for applicants who have spent significant amounts of time outside Australia (including recent arrivals) may not uncover robust evidence of criminality or security concerns overseas
- the criminal records against which backgrounds are checked depend on the consistency, thoroughness and speed with which all State, Territory and Federal courts provide information on their custodial verdicts to databases
- spent convictions are treated differently by different jurisdictions
- the CrimTrac database includes data on State and Territory convictions, but the AFP has to seek details of the convictions from the jurisdiction concerned
- the CrimTrac database does not include data on criminal charges laid or criminal associations
- the system for criminal background checking will not necessarily register the fact that a holder has done something since obtaining an ASIC that would have made him or her ineligible when first applying, because there is no 'live' system for updating criminal records, no ongoing consent to check, and new checks are only required when ASICs are reissued (every 2 years)
- though no issuer of an ASIC can admit an applicant who has failed the national security background check, different issuing authorities can have different standards on other criteria, so that even at a single airport an applicant can be rejected by one employer and given an ASIC by another on the basis of the employer's assessment of a criminal record
- issuers have noted that they are having difficulty in interpreting criminal history assessment criteria
- already on the way out are 'grandfathering' provisions for existing ASICs, which had meant the carry-over of ASIC holders' cards based on less stringent background checking
- there are security anomalies present at some airports because of the joint military and civil management arrangements. Military personnel do not wear ASIC cards, yet have access to secure airside areas. In some cases boundary lines are poorly defined and unsecured.
- among the 188 ASIC issuing bodies, there is no central list maintained of everyone who holds an ASIC

- ASIO and criminal background databases are not co-located, and there is no central body that can access all relevant databases
- it can take up to eight weeks for a background check to be completed
- the Australian Crime Commission's ACID database includes broader material on criminality such as criminal intelligence and associations, but data are not input routinely, consistently or in a timely manner by every jurisdiction or by Customs. The ACC is working with Customs to develop automated arrangements to transfer Customs intelligence into ACID, as presently exists with the AFP, and this should be expedited. Similar arrangements need to be expedited with jurisdictions that are not doing so.
- many people are eligible for Australia-wide ASICs that are currently viewed as providing generalised access to secure airside areas
- there is no 'fit and proper' person test applied to ASIC applicants who may have criminal associations and backgrounds that are not reflected in convictions
- required training for ASIC holders is minimal and inconsistent among issuers
- biometrics such as a fingerprint are not incorporated into ASICs
- ASIC passes themselves are often difficult to read unless up-close and the coloured background (red or grey) can make CCTV reading at night problematic
- supervised access may be granted using a Visitor Identification Card (VIC) in the absence of any background check; this can be a problem for security, recruitment and the functioning of an airport/airline (VIC holders are meant to be accompanied by an ASIC holder at all times but this may not always occur)
- on-airport employers such as security firms are using part-time and casual staff for sensitive tasks like screening duties, in advance of obtaining ASICs
- contractors for security and other on-airport roles are not proactive in seeking ASIC cards for their staff ahead of likely postings to a security controlled airport

- procedures and penalties for losing ASICs or for failing to return them when a holder ceases employment are insufficient to see the system respected.

36. Once an ASIC is issued, many take the ASIC card to be a general access card, rather than merely to be an indication that the holder has had a background check to enable potential entrance airside at an airport. Workers with ASICs can be reluctant to challenge whether other ASIC holders actually belong in a particular place at a particular time.

37. These symptoms go to the heart of another weakness in the current ASIC regime, which is the confusion around its function as (a) a background checking process; and (b) an access control measure. This partly reflects the evolution of the ASIC regime from its creation. The recent decision of the Australian Government to commence airside inspection of non-passengers reflects similar moves to tighten airport access control in the international community, including through ICAO. This represents an opportunity for the Australian Government, airlines and airports to reassess access control systems for major airports as well as background checking procedures.

Physical security

38. Currently 186 Australian airports are required to have security programs. So it is not feasible to make a universal statement about physical security that encompasses all of them. But it is necessary to make a number of general observations about shortcomings in this area.

39. While regional airports conducted security risk assessments to inform their Transport Security Programs, and while the CTFR airports have funded their own security risk assessments, the Review has found inconsistencies and shortcomings in the methodologies and approaches that have been employed. One notable failing is a simple inability to use the approved Australian and New Zealand Standard for Risk Management. As a result, the final assessment on the risk of terrorism occurring at regional airports could be exaggeratedly high, a rating inappropriate across the full range of regional airports. Similarly, some of the airport security risk assessments were mostly 'consequence' driven, including that prepared by ASIO's T4, which is arguably inconsistent with AS/NZS4360:2004. This could result in risk aversion rather than risk management.

40. CCTV is effective as a deterrent to illegal or dangerous activity; as a real-time monitor; and as a post-event source of

information on what transpired. But it appears that all too frequently the effectiveness of this tool is underplayed, even undermined, at airports. Much of the existing CCTV equipment is deployed for purposes other than security. Some cameras do not work, and have gone unrepaired for some time. Manning of monitoring screens can be hit-or-miss. Operating skills are not always high. No regulated standards exist for how and how long CCTV footage is to be retained. The latest digital technology is frequently not used, nor is there evidence of widespread integration of CCTV with Electronic Access Control Systems (EACS) or Electronic Intruder Detection Systems (EIDS). CCTV systems are run by different bodies, often without any coordination or cooperation, so that wasteful duplication of coverage is common and, despite ongoing improvements, many areas of concern simply remain uncovered. The exchange of information and the capability for mutual assistance among various agencies with CCTV capability is currently inhibited.

41. An established newer technology such as automatic number plate recognition (ANPR) is currently not used at Australian airports.

42. Allegations of poorly-functioning or even inoperative screening devices and of lax or poorly-trained screeners have been made. Mistakes do occur, and prohibited items will occasionally make it through: this is inevitable as long as human personnel are responsible for monitoring the technology because they can become fatigued, bored or distracted. But this is not an excuse for doing better. In addition to better training, there is a case for greater integration between screeners and AFPPS staff and between screeners and Customs.

43. Freight and mail present particular challenges. Much of the packing and gathering of these is done away from airports, with the ready-for-flight containers then taken by vehicle into the airport. Cargo shipped by a Regulated Air Cargo Agent is security cleared in accordance with the RACA's Transport Security Program before it is loaded aboard an aircraft but 'clearance' is largely a paper exercise and no physical screening of air cargo is currently mandated. Cargo shipped by other than a RACA is subject to security clearance in accordance with the TSP of the relevant airline. QANTAS screens all cargo for their international flights before it is loaded aboard aircraft, and a proportion of domestic cargo. That standard is not maintained for all international operators or for all domestic flights. Nor, except for cargo coming into Australia from abroad, is screening

done for contraband other than explosives. So the air freight system clearly has the potential to serve as an easy conduit, within the country at least, for the transfer of drugs, other illegal commodities or large quantities of money meant for laundering.

44. Unmanned, undermanned, or poorly-equipped access points to restricted areas both inside and outside terminals clearly represent weak spots. Abuse, misuse, or false use (including tail-gating) can occur with obsolete or unsophisticated swipe-card systems. A thorough inspection for contraband of the contents of each vehicle entering and leaving the secure area would prove oppressively expensive, and probably so time-consuming that airport functioning would be seriously impaired. Isolated guards at isolated posts sometimes struggle to fix full attention on what come to be mundane and repetitive tasks, and can allow unwarranted liberties to visitors or workers that they have come to know.

Border controls

45. While the Review has not examined border controls at airports in any detail, it is of the opinion that these are generally very effective. This includes both the roles of DIMIA and the roles of Customs including Air Border Security officers. However, terrorists and criminals may take advantage of the large number of false or altered travel documents in circulation world-wide. Passengers with multiple legal passports also present concerns because travel to potential terrorist training areas may not be able to be tracked easily, especially when names on different passports are not identical.

46. Emerging technology, such as Smartgate, may provide real efficiencies and more rigour in screening incoming passengers. Improved machine-readable passports will also assist. DIMIA is also in the process of developing and deploying an Entry Documentation capable of detecting fraudulent or otherwise suspect travel documents presented as part of the visa application process. In September 2005, DIMIA expects to commence the pilot of an APEC Regional Movement Alert List (RMAL) initiative. RMAL checks passenger travel document details against the Australian and United States' passport databases, to detect the use of lost or stolen passports by passengers traveling between these two countries. This APEC-sponsored pilot will be extended to New Zealand in November 2005, and then to other APEC countries.

Regional aviation

47. It is neither practical nor desirable to expect 100 per cent security at regional airports. The sheer diversity of Australia's regional airports makes the challenge of common standards of security an impossibility. Any protective security enhancements should be undertaken in accordance with a local threat and risk assessment and not instituted on the basis of what is sometimes media-driven scaremongering.

48. However, the Review noted the vulnerability of current arrangements as they relate to unscreened passengers on some regional regular public transport aircraft arriving at major airports such as Sydney and Melbourne with access to the apron and parked jet aircraft prior to screening. The Review also noted some inconsistencies in the application of risk management reviews at some regional airports. Frustration arises on the part of regional airport management through a perceived failure by officials to consult sufficiently about regulations and their implementation, as well as insufficient Commonwealth support for security education, training and administration.

7. Recommendations to Strengthen the System

I Information sharing

1. The present system of information sharing in and around aviation security is completely inadequate for the demands of our time.

2. Some change can be achieved through effective leadership, especially in bringing to an end procedures and practices which inhibit the sharing of information. But more than that is necessary. Legislation and regulations can also operate to prevent information sharing. The Review encountered first-hand the barriers to sharing information and intelligence set up by legislation such as section 18 of the ASIO Act, section 16 of the Customs Administration Act, and section 51 of the ACC Act. Privacy legislation also appeared to constrain the sharing of material among agencies and the private sector even when it was needed in the interests of national security and thwarting serious crime. Important Customs intelligence reports shared with the Review dating from 2000 to 2004 were in line with the 2003 report on Sydney Airport that had been provided without authorisation to *The Australian* in 2005 but it was not clear that they had been shared in a timely manner, if at all, with other bodies with a legitimate need to know. While the Australian Government has encouraged greater cooperation and sharing of security information with the private sector and improvements have been made (Annex 3), there is significantly less sharing than in countries such as the United Kingdom (Annexes 8 and 9) which have been exposed to terrorism for decades. The Review was also made aware of Police operations and investigations at both State and Federal levels that were not shared with others in the airport security community with a need to know.

I. It is recommended that a thorough examination of legislation and regulations on the sharing of information, both among government agencies and between government and the private sector, be carried out by the Attorney-General's Department, in collaboration with States and Territories and the private sector, with the aim of identifying and removing elements

which prohibit or inhibit the flow of information needed to counter crime and terrorism which threaten the aviation sector.

II Threat assessments

3. Intelligence is the first line of defence against terrorism and crime at airports, and it is a line that needs strengthening.

4. The collection and the processing of information on potential action by terrorists must be systematic and professional. Problems do exist with the frequency with which assessments are made and with dissemination of the conclusions reached after information is assessed. Obviously, national security Threat Assessments related to a specific or immediate concern, including in the aviation sector, must continue to be issued in a timely fashion and distributed immediately to those with interests at stake. But some substantial improvement must occur with regard to the sectoral Threat Assessments which from time to time provide information and overall judgments on the threats to the aviation industry as a whole.

5. ASIO's aviation-related Threat Assessments are fundamental to the construction and bolstering of defences against terrorist dangers, because it is on the basis of these that all others connected with the aviation industry prepare themselves systematically to act. So it is essential that these Threat Assessments be issued regularly and be relevant to airport-specific situations, and that their major messages receive as wide a distribution as possible, particularly through Federal and State police chains of command and the revised Airport Security Committees.

6. The risks to intelligence sources or intelligence-gathering methods may mean that full Threat Assessments may go to only small groups of security-cleared people in government. But sanitised versions of these reports, edited to remove risks to sources and methods but still including the essential evaluation of the dangers to the aviation sector from terrorism, should be available on a regular basis to a wider readership. The key judgments in those reports must be made clear to those holding security-responsible positions in the industry. This should occur through the Office of Transport Security in DOTARS.

II. It is recommended that the National Threat Assessment Centre prepare and distribute general national security Threat Assessments on the dangers posed to aviation and airports on a regular basis, and at least quarterly.

III Criminality assessments

7 There are reasons why the Australian Crime Commission's effort to produce general national criminal threat assessments cannot be guaranteed to mirror exactly the terrorism-oriented system culminating in ASIO Threat Assessments, particularly those directed at the aviation sector. Effective criminal intelligence collection methods and their results can differ from place to place, making comparisons of data less reliable. And criminals, criminal organisations, and criminal methods are likely, to a degree, to be location-specific, making any general judgments about dangers to airports as a group less useful than general judgments about the threat from terrorism.

8. But there is no reason to be content with the present situation. For, as things stand, many participants in the aviation industry, including such key elements as airport operators and police, admit they do not know enough about crime and criminality at airports to know what kind or level of problems they have, or sometimes whether they have a problem at all.

9. The way to address this is head-on. The gathering of publicly-available and covert information on criminal activity at and around airports must be boosted. Reporting of airport crimes must be collected, and presented in such a fashion that data can be compared across the board. Collation and analysis must be done, both for individual airports and for the sector as a whole. And conclusions reached, again both for individual airports and for the sector as a whole, must be disseminated to those responsible for airport security and policing, so that all of them have the best possible awareness of the dimensions of the criminal problems they collectively face.

10. While it is unclear whether centralised processing and analysing of data will yield a report on airport criminality as authoritative as a Threat Assessment on aviation-related terrorism, the advantages of a centralised system producing general reports are clear: a single data base, preferably utilising the ACC's Australian Criminal Intelligence Database; development of a professional analytic team capable of applying similar methods across the board; a capability for in-depth comparisons which would not be attainable under current arrangements; and the ability to service aviation security officials as they sharpen their own methods for understanding and combating crime.

11. The place to locate this centralised capability is the Australian Crime Commission, the nation's primary criminal intelligence agency. A unit should be set up in the ACC to manage all

intelligence matters connected to criminality in airports and in the aviation sector on an ongoing basis.

12 This unit on aviation and airport criminality should be properly staffed to perform all the key intelligence analysis functions. It should receive all available reports, including those derived from covert sources, on aviation- and airport-related crime and criminality, from the Australian Federal Police, State and Territory Police forces, the Australian Customs Service, the Australian Quarantine and Inspection Service, other appropriate government agencies, and the private sector.

13 The unit should also obtain relevant details of threat and risk assessments undertaken by Airport Security Committees. It should follow up those reports by requesting further information where necessary. It should store, collate, and analyse those reports against a background of publicly-available information. And it should produce its own reports, including, at least quarterly, an Aviation and Airports Criminality Assessment, for distribution to appropriate agencies. Sanitising of reports will be necessary to protect sources or methods, and this should be done, as with ASIO Threat Assessments by the originators and in consultation with OTS. What is important is getting developing knowledge about criminality in the sector communicated to those who need it in a timely manner.

III. It is recommended that there be established within the Australian Crime Commission a unit on aviation and airport criminality to collect, collate, and analyse relevant information on criminal behaviour, and to produce regular reports, including Criminality Assessments at least quarterly.

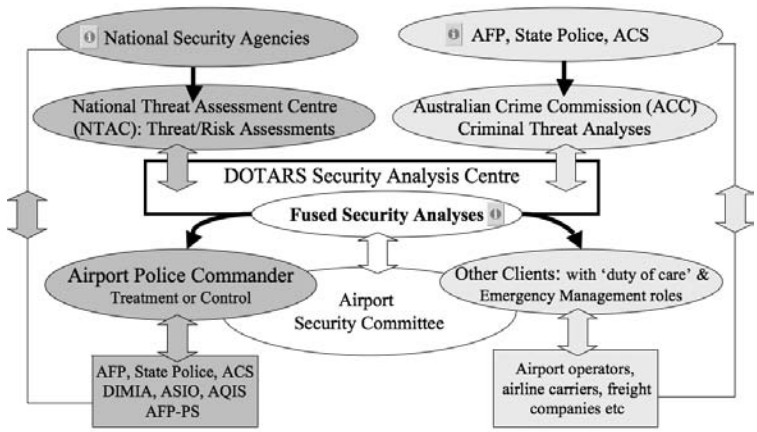
IV Disseminating information

14. Even sanitised, an ASIO Threat Assessment or an Australian Crime Commission Criminality Assessment on aviation and airports might still have to be too highly classified for more general distribution. ICAO recommends (Annex 17 paragraph 2.1.4) that each Contracting State should ensure appropriate protection of aviation security information. ICAO also has a Standard (2.3.5) requiring suitable protection and handling procedures for sensitive security information affecting other Contracting States to avoid inappropriate use of disclosure. But the key judgments in those assessments would clearly help security-responsible authorities at airports and in the aviation business to get a firmer grasp on the issues confronting them. So might other valuable information contained in those

assessments which could be disclosed without risking intelligence sources.

15. What is needed is a frequent and regular report distributed more widely at airports and in the aviation industry which takes the gist of intelligence assessments, and combines those essential messages with other useful information processed from public and private sources. The aim of this type of report would be to heighten and broaden awareness of the dangers facing the aviation and airports sector as a whole, and to strengthen the conviction among all concerned that they are working together against common foes.

FIGURE 1:
Airport security information and intelligence flow schematic



16. A report potentially similar in nature to this already exists, and is issued by the Security Analysis Section in the DOTARS Office of Transport Security. But that report in its present form is too general and appears too infrequently to serve the purposes intended here: the timely sharing of information and ideas, and a catalyst to strengthen cohesion within the security community at airports.

17. Rather than initiate an entirely new process or create a new body, the Security Analysis Section should be upgraded and be reinforced with a stronger analytical and reporting capability. The area should receive finished intelligence assessments relevant to security and crime in the aviation and airports sector from the Australian Security Intelligence Organisation and the Australian Crime Commission. It should combine the

judgments and insights in those intelligence assessments with other analyses and information available into reports updating the dangers posed by terrorism and criminality to Australian aviation interests. And it should provide these reports in a timely and regular manner, at least quarterly, to appropriate authorities at Australian airports. The upgraded area should also obtain and review ongoing threat and risk assessments made by Airport Security Committees.

18. This reporting regime could usefully be expanded to include the frequent provision of unclassified and open-source material relevant to airport and aviation security, critical infrastructure protection, and airport policing as a way of familiarising all concerned with the process of receiving and assessing terrorism and criminality information. In a similar vein, the reports could also include information relevant to international developments, including information and intelligence about last ports of call and incoming flights, and training and related capacity-building projects with neighbours in Asia and the Pacific. And this would also be a system with clear applicability to the maritime and rail industries as well.

IV. It is recommended that the Security Analysis Section within the Office of Transport Security in the Department of Transport and Regional Services be given additional analytical and reporting capability. Its tasks should include producing regular reports on security issues facing Australia's aviation industry and airports and to disseminate them in a timely fashion to those in the industry with a need to know, with a reciprocal feedback loop. This model is likely to be applicable to Australia's maritime and land transport industries.

v Airport classification

19. A one-size-fits-all approach to security arrangements clearly is inappropriate for Australia's airports, ranging as they do from massive international facilities employing and transporting tens of thousands of people daily to tiny airports where activity is sporadic. In its next amendment, Annex 17 to the Chicago Convention is expected to highlight further the importance of risk assessment at individual airports.

20. Governments are responsible for policing and for responding to terrorist events at airports. There is thus a need for clarity and agreement between airport operators and governments about how those responsibilities are to be fulfilled, and how measures to fulfil them fit in with operators' plans. It is not reasonable for

each airport to determine its own policing and security arrangements unilaterally.

21. Some classification of airports has occurred, into CTFR airports, other airports with jet passenger services, and the remaining smaller security-controlled airports. Rightly, the larger and more complex airports are required to have stronger security facilities and more intricate security arrangements, not least because they are likely to be more attractive targets for terrorists, as they are for criminals.

22. There are difficulties with this *de facto* classification arrangement. It is potentially static, while the world of aviation is not. And the boundaries between the groupings are not clear, particularly in the case of the differentiation between CTFR airports and others serviced by passenger jets, where it is not always obvious to all concerned why or when an airport might move between classes. Further, there is the issue of non-jet regular passenger transport aircraft without screened passenger carry-on luggage landing at major airports such as Sydney or Melbourne and walking (or being bused) on the apron.

23. Because the manpower and financial commitments involved in being a CTFR airport can be high, it is necessary to be able to determine under what conditions an airport qualifies to become, or perhaps ceases to be, an airport where CTFR capability is needed. Obviously, such factors as international connections, passenger numbers, cargo value, the frequent presence of political and business leaders, and the number of aircraft over-nighting or undergoing maintenance must play a part in this determination, because it is these that will serve to make an airport a more valuable and more likely target for terrorists and criminals. But at present there is neither transparency nor accountability connected with designating a facility as a CTFR airport. Some non-CTFR airports are increasing their business rapidly, while some CTFR airports are facing declining business or perhaps, objectively, should not have been designated as a CTFR airport in the first place. It is currently unclear how or under what circumstances change can or should be made to the present group of 11.

24. This overall issue of classification or designation is critical because:

    - of the way in which the vulnerability of the entire aviation industry can be affected by weak spots
    - the ability of particular airports to respond to crises can be altered

- of what high additional costs (screening equipment and the personnel to work it) can mean to some airports, and
- in the case of CTFR airports, that designation not only means having a CTFR contingent on the spot but also means that other security-oriented commitments (an Airport Police Commander, liaison officers from various agencies, a permanent community policing presence and a joint intelligence cell) will come on line.

25. Under these circumstances, it is necessary to have tangible criteria for differentiating among the various classes of airports. It is also necessary to have guidelines for the movement of airports from one classification to another. And review must occur to ensure that an airport is in the right class. Because of the cost involved in moving into or out of CTFR status, that review should occur regularly, but barring exceptional circumstances, not frequently. However, in the opinion of the Review, the status of Avalon Airport should be reviewed immediately.

V. It is recommended that criteria be established to determine under what conditions an airport should become or cease to be a Counter-Terrorism First Response airport, and that the Department of Transport and Regional Services be required to review CTFR airports and the major non-CTFR airports on a regular basis and at least once every three years so as to determine whether their classification is appropriate.

VI Airport policing

26. A large measure of the uncertainty surrounding everyday security and criminal matters at airports is caused by the disconnect between those units charged with CTFR responsibilities and those who have the tasks of 'community policing' and of investigating crime. The AFPPS officers performing the CTFR role do so, in the judgment of the Review panel, with varying degrees of competence and professionalism. But many at airports expect more of them and cannot understand why these uniformed officers do not participate fully in handling crime or breaches of the peace. The fact that AFPPS uniforms display 'Police' on jackets and caps reinforces in the minds of the public the belief that these are regular police officers. But in terms of their constitution and powers, they are not.

27. Likewise, employees and managers at airports frequently cite a worry that community policing at their workplace, meant to be performed by the local State or Territory force, is seemingly

neglected because that force has more pressing work elsewhere. Some State and Territory Police indicate that their interaction and communication with the CTFR authorities would be smoother, both in normal times and at times of crisis, if they were dealing with sworn officers with full policing powers. And not only do AFPPS officers not have full policing powers, in some cases there is uncertainty even among security personnel at airports about what powers AFPPS officers do have.

28. The policing arrangements in Australia are informed by the Constitutional settlement of 1901, under which the States continue their responsibility for criminal legislation and policing and to which there has been added the establishment of a Commonwealth Police Service, now in the form of the Australian Federal Police. Consequently the Review has had to consider, amongst a range of options, whether the AFP should have the sole responsibility for the policing of the 11 CTFR airports or whether the function could and should be transferred entirely to State Police, or some hybrid arrangement.

29. Policing at airports has one major goal: to ensure that the airport and its immediate and surrounding environs remain safe for those employed there, for those travelling to, from, or through the airport, and for those using the facilities there. To achieve this goal, there are three major policing roles:

    - community and traffic policing
    - confronting crime, and
    - airport crisis response.

30. Different duties and responsibilities are associated with these roles in the different zones at an airport: the airport approaches, the outside vantage points, the landside areas that come under the purview of the aviation industry, the terminals themselves, and airside. But the key element in this era is the need for policing authorities to take responsibility, at least initially, for coordinating emergency response services. It is this function, even on its own, that makes imperative an immediately available police presence at major airports.

31. At present, the Commonwealth pays only for a proportion of the CTFR presence at eight of the 11 CTFR airports (including the position of PSLOs) and airport operators pay the remainder. However, counter-terrorism first response is clearly a national security function. While the Commonwealth paid for uniformed and plainclothes policing at major airports in the 1970s and 1980s, it vacated the field ahead of obtaining State and Territory

agreement to take on the role with appropriate funding (see page 41 above). Consequently, States and Territories chose to provide a police presence at airports only when it suited their other priorities.

32. The Review took account of the opinion of the Australian Federal Police that they did not currently have the capability to undertake a 'community policing' role at CTFR airports. Nevertheless, the Australian Government does have specific responsibilities for aviation and airport security which cannot be ignored. The States also have responsibility for the presentation of life, property and the environment and hence deal with crime, emergency response and terrorist events in their jurisdictions. The Review was also cognisant of the submissions and views of State and Territory Police and their Ministers (and the impasse noted at page 41).

33. International experience clearly demonstrates that policing at major airports is a special skill for which the police need to be appropriately trained. The crucial policing functions at major airports include the provision of a public reassurance role, a general policing presence as well as the prevention and investigation of crimes and offences, keeping the peace, deterring and responding to terrorism and other emergencies.

34. It would be possible, for example in the case of NSW, for the Police of that State to assume all policing functions at Sydney Airport. But this might not be possible elsewhere. Indeed, it was made clear that some other States did not want to assume this responsibility, especially the CTFR function, even if the Commonwealth paid. The AFP brings substantial investigative skills that are relevant to the threat of security and counter-terrorism at the major airports, but it does not have the role of interfacing with the hinterland community surrounding an airport and is thus dependent upon a relationship with the State Police. This dependence would be even greater if there was a terrorist event requiring a smooth transition of command from the AFP to the State or Territory Police.

3.5 The Review therefore comes to the conclusion that the only practical and effective way to rectify the situation is through three major steps:

- First, and the key to a more effective system of policing, there must be an Airport Police Commander appointed to each CTFR airport, who will be responsible for all police functions at the airport. This Commander must be a senior police officer, holding the rank in the Australian Federal

Police appropriate to the size of the command at the airport[4]. The Commander should be selected by a panel including senior police officials from both the Australian Federal Police and the State or Territory in which the CTFR airport is located and a senior official from an appropriate Australian Government department (eg. the Inspector of Transport Security in DOTARS). In the event that the best officer for the job is an officer in a State or Territory force, that officer should be seconded to the AFP for the length of the posting at the airport, normally for five years.

- Second, a permanent State or Territory Police unit must be established and based at each CTFR airport under the operational command of the relevant Airport Police Commander who will be responsible for selecting the officers. The size of this unit can vary: larger at busier airports, smaller at the less busy, with the exact size to be determined after a proper threat and risk assessment. But the unit must be made up of sworn officers, trained to include the particular policing skills needed at airports. And the contingent of airport police officers must be 'ring-fenced': assigned specifically to the airport so that they cannot be called away from their airport duties whenever their home State or Territory Police superiors think they could more usefully be employed elsewhere. The appropriate commitment for an officer at the airport is probably three to five years, along the lines of other police postings. Existing State or Territory Police uniforms would continue to be worn. Airport police would be able to take extended leave or seek promotion in the usual way within their home service, provided they were backfilled by suitably competent and trained replacements.
- Third, the powers of the AFPPS contingent at airports, as well as those of the AFP, the Airport Police Commander, the relevant State and Territory Police force, and the Australian Customs Service, must be clarified and enhanced. At the least, all of these must have the power to halt, inspect, and

4 In the opinion of the Review, the AFP rank structure should be unambiguous and in line with police forces around Australia and internationally. This should apply across the AFP and may assist in further enhancing its credibility with State and Territory Police forces compared with AFP use of the non-hierachical 'Federal Agent' nomenclature.

hold persons, goods, and vehicles in, coming into, or exiting the airport, including adjacent roads and parking areas. Where necessary, legislation must be reviewed and revised at Commonwealth, State and Territory levels to ensure powers are comprehensive and harmonised.

36. These measures would ensure that Australia was in line with the Standards for both national and airport organisation set out in Chapter 3 of ICAO Annex 17, particularly Standards 3.1.8 (availability of resources at each airport) and 3.2.5 (deployment of resources to each airport to deal with unlawful interference).

37. The Airport Police Commander (APC) will lead a threat and risk assessment process which determines the appropriate size of the policing contingent at the CTFR airport where he or she will be based. The APC will control the operations of the contingents of Australian Federal Police, the State or Territory Police, and the Australian Federal Police Protective Service based there. The APC will work in collaboration with the Australian Customs Service, Australian Quarantine and Inspection Service, Department of Immigration and Multicultural and Indigenous Affairs, Department of Transport and Regional Services, and any other government-agency staff based at the airport. In the event of a terrorist incident, the APC would assume command of all airport-based officers. And the APC will consult with, and establish through regular exercises and training, an effective working relationship with the appropriate police commanders in the State or Territory in which his or her airport is located.

38. To enable Airport Police Commanders to do the job fully as they confront the possibility of terrorism and serious crime at airports, it will be necessary that each have working for them a special body, a multi-agency Joint Intelligence Cell. This Cell should have, at the least, representatives from: the Australian Federal Police, the State or Territory Police, the AFP Protective Service, the Australian Customs Service, the Australian Quarantine and Inspection Service, and the Office of Transport Security from DOTARS. It should have a built-in analytical capability, in the form of one or more full-time analysts, trained in police-intelligence analysis and reporting. And it should have, as *ex officio* members, representatives from the Australian Security Intelligence Organisation, the Department of Immigration and Multicultural and Indigenous Affairs, and the Australian Defence Force when those organisations have duties at the airport.

39. The tasks of this Joint Intelligence Cell should include: gathering all available information on illegal activity and on planning for such activity at the airport; collating and analysing that material to discern patterns, intentions, and capabilities of those who would threaten security and order at the airport; initiating measures to fill in gaps in the Cell's knowledge base; and planning measures to confront threats and risks. This Cell will play a central role in sharing information and intelligence with key partners (cf UK MATRA in Annex 8) including the revised Airport Security Committee, ASIO, the ACC and the OTS.

40. To break the impasse explained at page 41, because of the national importance of security at Australia's major airports, and because all policing, both CTFR-related policing and community policing, will come under the command of a senior Australian Federal Police officer (substantive or seconded), all funding for policing at these airports should be an Australian Government responsibility. The funds allocated to support appropriate policing at these airports should also be ring-fenced: marked off as a separate item, and protected from diversion. The funding would include all CTFR personnel, the members of whom may be able to be reduced when full and integrated policing arrangements are in place, depending on threat and risk assessments. Commonwealth funding for community policing at CTFR airports, plus the intelligence analysis function and an Airport Police Commander with appropriate deputies to enable up to 24 hour coverage, is estimated by the AFP to cost $117.4 million per annum. The full cost of CTFR would be in addition. Movement from a base agreed by the AFP with the Australian Government and the relevant jurisdiction's Police force should be determined by changes in airport threat and risk assessments.

VI. With regard to policing at airports, it is recommended that:

- **the position of Airport Police Commander be established at each CTFR airport, to be filled by a senior police officer holding appropriate rank in the Australian Federal Police but who may be seconded from a State or Territory force. The Commander's responsibilities will be to command the general policing presence, which will include the delivery of all policing functions such as public reassurance and prevention, the proactive and reactive investigation of crimes and offences, keeping the peace, as well as deterring and responding to terrorism**

- **the Airport Police Commander be selected by a panel including the AFP and the Police force in the jurisdictions in which the airport is located**
- **the Airport Police Commander work in collaboration with other government agencies assigned to the airport, and supervise the work of an appropriately staffed Joint Intelligence Cell**
- **an appropriately sized State or Territory Police contingent be posted to each CTFR airport, and comprise police officers selected by the Airport Police Commander and specially trained for airport duties and assigned solely to tasks at the airport**
- **all police, AFPPS and Customs officers deployed to an airport be given clear and unambiguous powers, including to stop, search, detain and arrest where necessary within the airport and adjacent roads and parking areas**
- **the Commonwealth provide ring-fenced funding for all policing functions at CTFR airports which includes the CTFR function and the general police presence**
- **legislation be reviewed to provide appropriate powers.**

VII Airport Security Committees

41. Reliance should continue to be placed on three of the main security pillars at airports, the Airport Security Committee system, the Transport Security Program, and the Aviation Security Identification Card system. But these need to be strengthened and supplemented if they, and effective interaction among them, are to work as they should.

42. Airport Security Committees, which bring together representatives of all agencies and businesses with an interest in security, vary enormously in effectiveness. This is so because they may have no strong leadership, too broad and inclusive a membership, and only limited access to classified information. As a result, a solid and purposeful exchange of information, leading to the design of effective strategies, actions, and their subsequent monitoring, which is the aim of the Committee, is uncertain.

43. What is needed is a more focused and integrated security committee system with more authority and an enhanced ability to share information. The way forward is to change the size, composition, and nature of the Airport Security Committee,

and to keep present larger groupings together as a re-badged Airport Security Consultative Group. This is more in line with Standards 3.2.2 and 3.2.3 of ICAO Annex 17 that require a security coordinating authority at each airport and a body to assist that authority with the implementation of security controls.

44. The Airport Security Committee should be chaired by the Airport's CEO or, if the CEO is unavailable, a high-level representative. It should have no more than ten members, who should include the Airport Police Commander, representatives of those government agencies with airport-security interests and capabilities (the Australian Customs Service, for example), and representatives of major operators at the airport (for example, a senior airline representative, a senior Airservices Australia manager, and possibly a representative of tenants at the airport). All of its members, including the Chairman, would have to undergo the security-clearance process, so that discussion of classified information related to security issues could occur. The tasks of the Committee would be to uncover and analyse threat and risk areas in security and to decide upon strategies and actions to address them and monitor their implementation.

45. The Airport Security Consultative Group would retain a key function of the existing Airport Security Committee: information exchange. It would be chaired by a senior representative of the Airport CEO, and would include either the Airport Police Commander or his or her representative, who would be in a position to relay the gist of the discussions and decisions taken at Airport Security Committee meetings. The Chairman of the Consultative Group and the police representative should be ready either to act on any problems raised at the Group meetings or to pass on to the Airport Security Committee any information raised that would be relevant to the deliberations and decisions of that more senior Committee.

VII. It is recommended that the Department of Transport and Regional Services require that the Airport Security Committee be refashioned at each CTFR airport to be a focused and strategic group, chaired by the CEO of the airport or the CEO's high-level representative. Its members, including the Airport Police Commander, are to be security cleared representatives of government agencies and major operators with security interests at the airport. Its tasks are to identify security threats and risks and to initiate action to address them and to monitor their implementation. The current larger existing Airport Security Committees at CTFR airports should be renamed Airport Security Consultative Groups.

VIII Monitoring risks

46. The concept of an overall Transport Security Program (TSP) for each airport, consistent with Transport Security Programs for the component organisations working at the airport, is a good one and entirely consistent with the requirements for written security programmes set out in Standards 3.2.1 and 3.3.1 of ICAO Annex 17. The concept itself reinforces the crucial point that security depends not upon a single organisation doing its job, but upon each pulling its weight and all pulling together. Another advantage is that in creating the airport's TSP, each organisation must review its responsibilities, renew its awareness of the responsibilities of others, and outline the measures it will be taking to improve its performance.

47. But a Transport Security Program is not without its problems, for a large airport in particular. It is too bulky to consult with ease and the TSP is too static to accommodate rapid change. What is needed is supplementation of the Transport Security Program with a more continuous, more flexible, system of planning and reporting on security issues. This system should feature a regular review of the security threats being faced by an airport, of the vulnerability of the airport's assets, and of the risks still faced despite mitigating efforts in place, and should then be aimed at putting in place strategies and action plans to address outstanding weaknesses (Annex 8). The ideal would be a monthly discussion, but review could occur more frequently if the security situation was changing rapidly.

48. This process should be conducted in and by the Airport Security Committee, be supervised jointly by the chairman of the Airport Security Committee and the relevant Airport Police Commander, and result in an agreed formal document at the end of each review. Copies of that document should be made available to the Department of Transport and Regional Services, to the National Threat Assessment Centre, and to the unit addressing aviation sector crime in the Australian Crime Commission.

49. The OTS in DOTARS, after collecting and reviewing these reports, should determine whether there are systemic weaknesses which need to be acted upon at more than one airport, and should be prepared to use the information collected to inform airports more widely about problems and the best practices for addressing them. Actions to remedy weaknesses should also be notified to ICAO as required under Standard 3.4.6. Also relevant is Standard 3.4.5 requiring, *inter alia*,

surveys to identify security needs. ICAO also recommends (3.4.7) that the effectiveness of individual aviation security measures be assessed by considering their role in the overall system. This data is likely to facilitate such an assessment. If, in initiating this process, Airport Security Committees need guidance and support, OTS should be prepared to assist.

VIII. It is recommended that the Department of Transport and Regional Services require that Transport Security Programs be supplemented by a more frequent system of reporting that ensures that airports regularly review their own security gaps and weaknesses and document the measures being taken to address them. Reviews of threat and risk should be undertaken by Airport Security Committees, with their reports collected and analysed centrally by the Office of Transport Security in DOTARS, in order to bolster the national effort to understand and counter threats.

IX Reviewing the regulatory regime

50. The *Aviation Transport Security Act 2004* provides a solid basis for security regulation of airports and associated activities. The Act and the *Aviation Transport Security Regulations 2005*, however, were developed with less than optimal consultation in order to be operative from 10 March 2005 and would benefit from a review with the aim of clarification and simplification. There is a danger that airport security could become focused on compliance with regulations rather than on the crucial preventative role through assessing threat and risks on an ongoing basis and mitigating these in a timely way. Regulation should encourage good outcomes through good systems and processes and through improved behaviour and culture.

IX It is recommended that the *Aviation Transport Security Act 2004* and the 2005 Regulations be reviewed by the Department of Transport and Regional Services to ensure that they encourage a culture of proactive and ongoing threat and risk assessment and mitigation and not a passive culture of compliance.

X Background checking

51. The Aviation Security Identification Card (ASIC) system has been under steady review and modification since its introduction as an industry responsibility in 1998. And throughout this Review the Australian Government has been considering further changes to help see that the system serves

what have become its two aims: ensuring that only fit and proper persons gain employment which involves entering workplaces in secure areas of airports; and helping to ascertain that only those with their own valid ASICs enter their designated secure work areas at appropriate times. The Review welcomes the deliberations under way addressing the awkward and complex issues connected with the ASIC system, and recommends a way forward that is consistent with existing (and likely future) ICAO material. For example, the current version of Annex 17 addresses the need for background checking, identification procedures, and the control of access to security restricted areas in Standards 3.4.1, 4.7.1 and 4.7.2.

52. The system for gaining an ASIC should be tightened further, through three broad reforms:

    - First, employers and potential employers, along with employees and potential employees, must recognise that they bear a significant responsibility to ensure the system works. Employers have an obligation to use an effective job-application process, including thorough checking with at least two referees, to help ascertain that a prospective employee merits serious consideration for a position in an industry where security is a top priority. All on-airport employers must be prepared to vouch for the validity and staff need for ASICs prior to seeking authorisation and to provide appropriate assurances as to the potential staff member's suitability. An applicant for an ASIC must be willing to undergo a potentially intrusive background check. Approval for background checking is required on an ongoing basis, and the applicant must agree to disclose any subsequent criminal investigations or charges as soon as they become aware of them. The applicant must also be ready to present strong proof of identification. In addition to standard identification certificates, a verifiable work history should be required, and fingerprinting (or other biometric technologies) should be part of the process of applying for an ASIC. The process will be best managed by a standard ASIC application form.

- Second, the screens through which an application passes should be uniform and of a tighter mesh. The process of checking an application against the applicant's background should be centralised and performed by a single agency with immediate access to continuously updated lists of ASIC applicants (including those denied an ASIC for any reason). The agency to perform this checking and maintain that data base should come

under the Attorney-General's portfolio, desirably entailing an expansion of the capability of the Australian Security Vetting Service (ASVS) in a new Division within the Attorney-General's Department with ready access to information on criminal records and politically motivated violence enabling the exercise of a 'fit and proper person'[5] test based not only on convictions but also broader patterns of criminal behaviour and substantiated significant criminal intelligence. The new central authorising body should also have ready access to DIMIA's databases. Existing ASVS checking should be integrated with the ASIC role to minimise duplication (ie public servants, police and ADF checking should be recognised and not unnecessarily repeated). However, most ASIC applicants will not require vetting interviews by the central authority.

- Third, development of an effective (accurate) and efficient (timely) 'fit for purpose' database will entail significant collaborative effort with the ACC, CrimTrac and any other relevant organisations in order to maximise access to information on convictions and criminal intelligence. The ACC's ACID database appears to offer the best platform to incorporate data on criminal intelligence and, in the future, convictions from each jurisdiction. ACID should also incorporate all relevant Customs data. This will require each jurisdiction to input data into ACID in a timely, consistent and complete manner. To establish the ongoing political will to do so is likely to require a clear decision by the Council of Australian Governments.

53. This Review also suggests that an inability to confirm the criminal history of an individual who has spent significant time overseas could be grounds for directing that an ASIC not be issued pending successful completion of such a check.

---

5 A 'fit and proper person' test would require the central authorising agency to assess all available information (including any automatic 'disqualifier' crimes) on convictions, charges criminal associations and the like and to issue either (a) a direction to an employer that an ASIC not be issued, or (b) advise that there is no reason for an employer and issuing body not to issue an ASIC. This would leave an employer with a discretion not to employ (or to constrain the employment, eg by not permitting an employee with a drink driving record to transport high consequence dangerous goods) anyone once the details of their criminal record became known. A less clear result (c) may require discussion between the authorising authority and requesting body.

54. It is acknowledged that there will be a significant time lag in the full implementation of the new ASIC system. Once available it should also handle maritime industry (ie MSIC) and other background checking. An integrated process of this kind would provide an ideal opportunity for the Government and relevant industries to review the coverage of background checking in the light of experience (eg whether all aviation industry employees should be subject to background checking, and/or whether airports below a certain threshold should be exempted on the basis that background checking added little value in small communities).

55. The background checking process should also be more stringent than merely running a name against a list of those disqualified because they are proven national security risks, recently-incarcerated criminals, or non-Australians illegally present in the country. Information, including substantiated criminal intelligence, held by police forces in Australia and related to patterns of less serious crime or to criminal association, for instance, should also be made continuously available to the central authorising agency and should be taken into account as the agency makes the determination whether the applicant is a fit and proper person to be employed in or around the aviation industry. Based on the central agency's 'reasonable' judgement as to 'fit and proper' person, this agency would direct card issuers either that they must not issue an ASIC or that they may do so if both they and the employer are satisfied as to the character, health and so forth of the proposed employee.

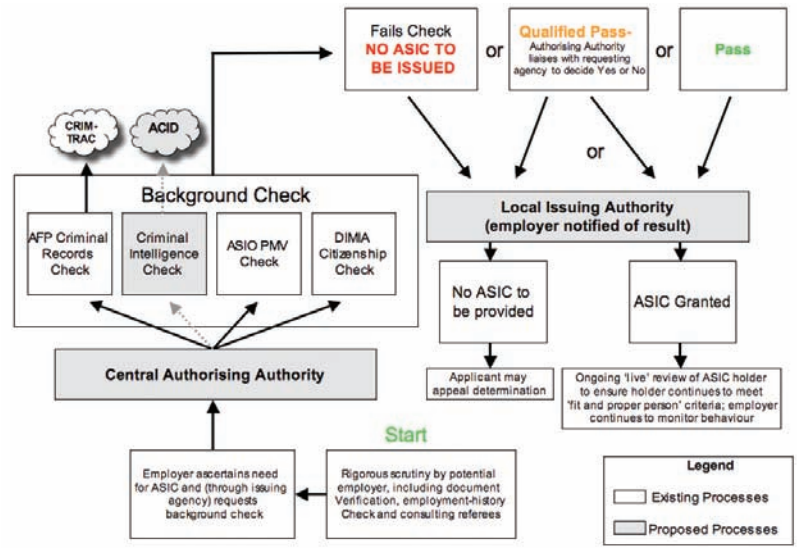
56. Card-issuing bodies would normally be each airport operator, with the addition of major employers such as QANTAS, Virgin Blue and Customs. The central agency should also hold a consolidated list of all those who have been issued with an ASIC and those who have applied in the past, a list that should be made available to law-enforcement agencies and to the Australian Customs Service when they have need of it. This is likely to require legislative amendment (eg re privacy law) which should occur in the interests of preventing terrorism and serious crime.

57. Natural justice for those who might have their applications for an ASIC denied by the central authorising agency requires that appeals to the Administrative Appeals Tribunal should be possible. For the system to be effective, however, it will be necessary for there to be a secure appeals process (consistent with section 38 of the Australian Security Intelligence Organisation Act 1979) in which not all information about a rejected applicant is made available.

58. Once the central agency advises the issuing authority that, based on its reasonable judgement, it has no objection to the issue of an ASIC, the required zones of access need to be agreed for the airport or airports that the applicant has a regular need to enter. Employers and issuing authorities should have an ongoing obligation to monitor their employees and alert the central authority if any significant concerns arise at the workplace (eg suspected financial difficulties, gambling, alcoholism or drug use). A flow chart broadly illustrating the proposed ASIC process is at Figure 2.

59. The system has to close off the possibility that applicants waiting for approval can repeatedly enter secure areas using a Visitor's Identification Card as though this were an ASIC. Clearly there is a need for a Visitor's Identification Card system: some items airside, for example, need repair or maintenance only infrequently, and those called on to do that work do not warrant an ASIC: they need only a Visitor's Identification Card which will permit them to be in the secure area while under the supervision of an ASIC-holder. But this system cannot be abused without risk. It is incumbent upon employers to manage their workforces so that their employees needed to get the job done are ASIC-cleared if they are to enter airside or properly accompanied, and it is incumbent on government to make a mandatory process of background checking capable of delivering timely and accurate results.

FIGURE 2:
ASIC approval process schematic



60. To improve the security functioning of the ASIC system once a card is issued, further steps need to be taken:

    - the central authorising agency should continue to monitor incoming information, and move to have an ASIC rescinded should a holder be guilty of an offence which would have denied him or her a Card on application
    - a mechanism must be found to ensure that ASIC holders return their card immediately when it is no longer required: the Review was attracted to the oft-repeated suggestion that the final wage payment to a terminating employee be conditional on return of the ASIC. Cards with magnetic access strips should, of course, be disabled when employment ceases
    - regular training must be provided to card-holders to reinforce their understanding of the proper use of an ASIC, to boost their knowledge of their responsibilities to help protect the system, and to ensure that they are aware that the card is only an indication that its holder is a fit and proper person for employment in the industry, and does not confer the right to access all secure areas at all times.

61. There are clear benefits in using a single card for identity and appropriate access, while limiting access to airside areas when a person has no requirement to be there. Use of a magnetic access strip on a single ASIC card such as through the MIFARE system used by QANTAS and at airports in Adelaide, Brisbane and Cairns (or more recent similar technology) is worthy of more general consideration at larger airports. This should be coupled with enhancements to the card itself that have boxes indicating the employee's role and the airside or landside zones that he or she may have access to. For example, there should be limited access to Customs-controlled areas, and this should be clear from, say, the card of a general aviation pilot's ASIC. (Figures 3 and 4 provide examples of possible ASIC background checked and non-checked access cards linked to airport zones.)

62. Improving the ASIC system is one area where Australia could benefit from the experience of others. Different countries, and even different airports in the same country, have different methods for checking the backgrounds of those involved in the aviation industry. The Canadian system, for instance, has been centralised for some time and is judged to be highly effective. As the centralised authorising agency recommended here moves forward, its officers should seek to discuss with the Canadian authorities lessons learned from the Canadian experience. And

the embedding of biometrics, such as fingerprints or facial-recognition characteristics, in the Card itself is also being used elsewhere and may be appropriate (eg, all 110,000 Changi Airport cards are being reissued in Singapore by the end of 2005, including to incorporate a fingerprint biometric). The system used for aviation should also be applied in the maritime sector and possibly to improvements in other areas, such as land transport.

X. It is recommended that the background checking process required to obtain and hold an Aviation Security Identification Card be further tightened and centralised in the Attorney-General's Department and that this should be harmonised with maritime cards.

FIGURE 3:
Proposed ASIC card based on zoned access

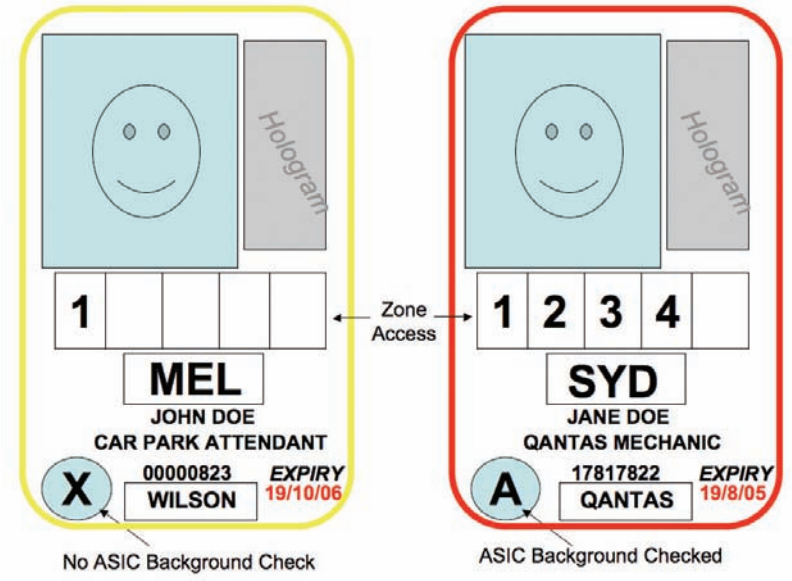
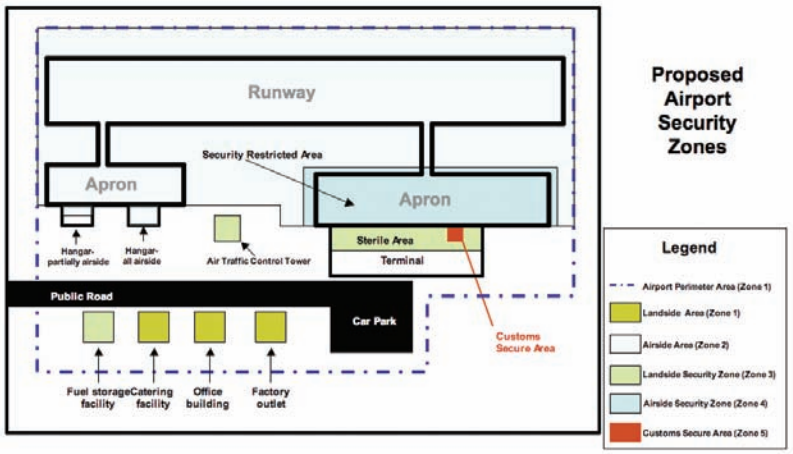


FIGURE 4:
Layout of an airport broken down into proposed zoned access areas



XI Physical security

63. Physical security equipment and arrangements at and around airports are being strengthened including following Australian Government decisions in June 2005. Much of the improvement going on is on the right track. Still, comment and recommendations for further improvement are warranted in some areas.

64. Controlling access to the secure sections of airports is another area where Australia can learn from examples and ideas developed overseas. At the urging of the Australian Government, airports here are already reducing the number of access points to airside. The Review applauds this development, and urges that further reductions be undertaken, if necessary by regulatory change. However, more still needs to be done to limit the dangers faced at the access points that will remain.

65. Tail-gating, where one person swipes a card to gain access airside and is then followed through by others, remains a problem at airports here. And instances can even occur where packages are tossed from landside to airside. In some countries, this is precluded by having every person entering airside at all points observed and required to have themselves and their possessions screened by walk-through metal detectors, x-ray machines, and hand-held metal detectors. In one place, anti-tailgating doors, activated by access cards, are being explored to address the problem.

66. The entrance of vehicles airside is a particular concern at some airports. In the toughest regimes, all vehicles entering need to

have satisfied the airport's standards beforehand, and then they must display visible permits, have their cabins, compartments, and undersides inspected, and have their drivers and any passengers screened and checked for access permission as they pass through an entrance point. Most Australian airports fall well short of this, though in some places 'air-lock' systems have been put into place to ensure that only one vehicle at a time can enter.

67. At the most security-minded of the major airports overseas, movement is toward integrated electronic access control systems (EACS) and electronic intruder detection systems (EIDS), incorporating verification of the authenticity of access cards to control entry. The trend is likely to see greater integration of EACS with CCTV and secondary biometric measures such as fingerprint, face or iris technology.

68. In addition, security guards are commonly stationed at each access point. At vehicle access gates (and perhaps on roadways outside the terminal), automatic number plate recognition (ANPR) technology can help screen for expected and suspect vehicles.

69. Obviously, the cost of implementing top-of-the-line measures at all entrance points at all airports would be prohibitively expensive, and the need for specific equipment and specific measures will depend upon the risk assessments done at airports here. But one theme that is becoming increasingly clear is the need to integrate all other measures of limiting and monitoring access with the use of Closed-Circuit Television, which should record all movements in and out of airside.

70. The Australian Government is already moving to embrace an advanced use of CCTV in public places, a move the Review most strongly supports. CCTV is proving itself ever more useful as a weapon against both crime and terrorism. It can with discretion constantly monitor vulnerable areas. Its presence alone can deter unwanted activity. And its use in forensic investigations is becoming clearer almost daily. Yet at many major airports in Australia, which are not only strong magnets for criminals and potential terrorists but also ideal sites for the employment of CCTV, the use of this tool is limited, and it is sometimes misused altogether.

71. This must change. At airports, standardisation toward the latest digital CCTV, and toward the length of time recorded material is to be preserved, is necessary. This is likely to require

regulation. Many more CCTV cameras must be deployed, not in the haphazard and add-on fashion which now marks their use at so many airports but rather in a planned and systematic manner to give full and continuous coverage in areas of concern, including terminals, access points, cargo areas, and baggage-handling areas. But more needs to be done than simply putting additional and more modern cameras in the right places. Monitoring must be done by people trained to a high level. And any obstacles, legal, regulatory, or customary, to coordination and cooperation in the use of the CCTV by police, Customs and public and private sectors security bodies in an airport must be removed. The Airport Police Commander should ensure that this occurs.

72. At Australia's major gateway airports, the Australian Customs Service has usually taken the lead in CCTV advancements, and it is Customs which should be chiefly involved in providing guidance for the more sophisticated use, retention, storage and back up of CCTV at those airports, both in international and in domestic terminals. It should also be incumbent upon Customs to ensure that it and the other security agencies at those airports use the CCTV systems there in a coordinated and cooperative sharing arrangement, in full consultation with the airport operator. Ways should be found to have the expertise developed at Customs in setting up and monitoring CCTV made available, with appropriate training, to other security controlled airports in Australia. This will require appropriate legislative changes and funding.

73. CCTV is not simply a stand-alone protector. When it is used together with other security technologies, such as EACS, EIDS, ANPR, and biometric systems, its value and theirs are multiplied. This is especially the case in and around airports.

XI. It is recommended that integrated Closed-Circuit Television systems be expanded and improved at Australian airports, and that, with the Australian Customs Service as the lead agency, arrangements be made to ensure CCTV standardisation, digital upgrading, storage, and fully coordinated use by Customs, police and security personnel.

XII Protective security screening and training

74. Screening of personnel, baggage, and cargo at Australia's airports is the responsibility of the airline or of the terminal operator, and is conducted by private security officers, usually contracted. The job is demanding. It requires not only some

expertise in the proper use of complex machinery but also long periods of focused concentration and the more-than-occasional deployment of people skills. If this job is to be done correctly, and the system to be safe, these officers must be background-checked, trained to an appropriate level, and tested frequently to ensure that their skills and their attention to detail do not erode, as is already a requirement of ICAO Annex 17 Standards 3.4.2 and 3.4.3 requiring training, certification, and the setting of performance standards for those implementing security controls.

75. Because of the importance of these screening personnel, and of the private security guards employed at larger airports, it is necessary that realistic but rigorous standards be set for employment in this field. And because of the national inter-connections in the airline industry, where screening done in one airport can have serious implications for an airport a great distance away, those standards should be uniform across Australia, and should apply to sub-contractors and part-time guards as well. Some States and Territories (NSW, the ACT and most recently Victoria) have already instituted licensing standards; the work done in preparing those could help in establishing a national licensing regime and be encouraged by COAG.

76. Now is the time to move to improve standards in this field. In the next few years, as more and more passengers purchase e-tickets via the internet and then check themselves in at airports, the responsibility of screeners will grow, because they will become an even more important line of defence against those who might cause danger on and to planes. In the same time period, rapid technological change in detection devices will demand extra efforts from screeners if they are to keep up to date.

77. If the need for training, for updating, and for exercises is important for screeners and private security personnel, that need is even more crucial for the police forces which will be stationed at major airports, including both the State and NT Police detachment and the officers responsible for CTFR.

78. Even before officers assume their positions at airports, they should have undergone full training in the specialised skills that airport policing and CTFR demand, including the use of the firearms they will have to employ in the event of a major terrorism-related emergency. Once they are working on-site, all airport policing personnel will need regular instruction periods

to ensure they are kept up to date on the latest protective equipment they must wear, on any weaponry introduced, and on the best methods of using their communications equipment, in addition to regular briefings on the problems of criminality and terrorism they might face in the course of their duties. And both the CTFR detachment and the State and NT Police based at the airport, including the Airport Police Commander and any staff, must go through regular exercises to ensure that should a crisis occur they can competently and confidently address it, knowing what their individual tasks are, how those individual efforts are coordinated with those of their fellow officers, and how the policing forces will work together with other elements already at the airport and with others as they arrive.

XII. It is recommended that the Attorney-General's Department work with State and Territory Governments to require that private security officers in the aviation industry, including those responsible for screening at airports, be background-checked, licensed, and trained to more adequate minimum national standards and that the Department of Transport and Regional Services require that there is a more comprehensive training programme for all security related airport staff.

XIII Access screening

79. A related and prominent weakness in security arrangements at airports has been the uncertainty and the uneven arrangements around the issue of screening of employees.

80. The questions of whether all or some employees should be screened, by metal- and other detecting devices and/or by frisk searching, as they enter and/or leave secure areas can be awkward ones. Some see screening as indicating a lack of trust. Some feel it is needlessly intrusive, or uselessly time-consuming, especially if their work compels them to move in and out of secure areas frequently during a shift. Some of the international attention currently being devoted to these issues is summarised in the Restricted ICAO Security Manual. The current version of Annex 17 already carries a recommendation (4.7.5) that non-passengers (and the items they carry) seeking access to security restricted areas should be subject to random screening in accordance with risk assessment carried out by the relevant national authorities.

81. Enhanced security must be the overriding concern when this issue is considered. No screening officer should be potentially subject to coercion, corruption, or exploitation of his or her

position because he or she has to decide whether to screen certain employees and exempt others from the process. And no staff should be exposed to corruption or coercion because they are exempt from screening. Also of high importance is a sense of total involvement with a team in which everyone, regardless of rank or uniform, is treated equally. With these uppermost in mind, it is best always to come down on the side of security. The only exceptions to screening should be hot pursuit, extraordinary emergency situations, or uniformed police and CTFR officers carrying weapons. Given the current number of staff airside access points at major airports that do not require screening, it is recognised that significant re-engineering will be required.

XIII. It is recommended that the Department of Transport and Regional Services prepare regulations so that airports ensure that all those entitled to enter airside secure areas at CTFR airports in connection with work responsibilities should be subject to screening each time they enter, and potentially subject each time they leave, the secure area.

XIV Cargo screening

82. Though Australia is well ahead of most countries in having some form of security regime for cargo carried by aircraft, the regime must be tightened further. The present system contains gaps and inconsistencies. It sees international cargo examined for contraband as it enters Australia, and QANTAS inspects cargo for explosives as it leaves the country. But cargo on flights within Australia is examined only at some airports and not all cargo is subject to physical inspection. This system does not prevent the shipment of drugs or illegal commodities and cash within Australia. Also, it has the potential to permit explosives and explosive devices on passenger aircraft. The Australian Government is already moving ahead with plans to tighten up the cargo-screening system, and this Review strongly supports extending that effort.

83. No country has identified a watertight system for freight which is also practical. Because much of the work of readying freight for shipping is done away from the airport, the ASIC system is inapplicable to the bulk of people involved in the business. Screening of every packet, parcel, and container as it enters every airport would call for a massive outlay for expensive equipment and then for high ongoing costs for the manpower to attend the equipment and maintain it, even though it might be used only sporadically at smaller airports. And resultant

delays would threaten to negate the major attraction of air-freight: the speed that attends it, and makes it all-but-indispensable if high value perishable items in particular are to be marketed.

84. Under these circumstances, risk management methods must be applied. The strongest feasible measures should be prioritised to prevent the most likely or the worst-possible of the negative outcomes. Other resources deemed appropriate are to be devoted to heading off less costly or less likely negative results. The reality is accepted that not every bad outcome can be prevented. But plans should be put in place to handle situations should such an outcome actually transpire.

85. In the aviation freight/cargo sector, this approach leads to one inescapable conclusion: where passengers are being carried and the risks are deemed to warrant passengers' checked baggage being screened, cargo carried on such flights must be screened.

86. For international flights departing Australia, this will mean greater powers, greater resources, and greater activity for the Australian Customs Service. It is that Service which should have the responsibility for security over export air cargo, a responsibility which is likely to entail:

- Government action to enable Customs to gain earlier reporting of cargo details and to impose stronger controls over licensed cargo depots
- the acquisition by Customs of additional x-ray equipment and sniffer dogs, and
- bringing more explosive trace detection technology to cargo depots and terminals.

87. For domestic flights, a similar regime presided over by appropriate authorities such as airlines and cargo handlers, using methods and equipment tested by Customs, will also have to come into force. The Review acknowledges that there are issues of establishing standards (methods, equipment, techniques) for the conduct of cargo screening. There is also the question of whether screening is best regulated under the Aviation Transport Security Act or the Customs Act which need consideration as part of implementation.

XIV It is recommended that the Australian Government require that the screening of cargo be expanded and include mandatory screening of all cargo on passenger aircraft where passengers' checked baggage is screened.

XV Regional airports

88. Regional and smaller airports in Australia face problems of their own. So does the general aviation sector, the thousands and thousands of private pilots who fly small aircraft for pleasure, or for private business and other purposes.

89. With regard to general aviation, this Review has some observations. The requirement now to keep aircraft locked when not in use has already helped address one earlier weakness. And the tightening of the background-checking for licensed and aspiring pilots, to the same standards and through the same central authorising agency as the process for the holder of an Aviation Security Identification Card, will strengthen the capacity of this sector to withstand dangers posed by criminals and terrorists. True, criminal elements facing tighter security measures at larger airports or in commercial travel might turn to general aviation as a softer option for transporting illegal goods or people. But countering such a move should be left to intelligence-driven general police work, and the coordinated use of CCTV and access control measures, where those are available at the entrances through which general aviation participants gain access to the tarmac, should assist in that police effort.

90. Regional and smaller airports demand more attention. Their importance in Australia should not be underestimated: in many areas they are crucial in sustaining the vitality of communities. Yet their operators face an awkward dilemma: they are aware that security measures are necessary to keep public confidence in air travel high, but the increased cost of security measures can threaten their very existence.

91. Those running smaller airports feel they have some security advantages over larger airports. Staff working there can be so few that they would immediately note the incursion of unauthorised personnel into secure areas. Retaining close and easy relations between airport operators and the police appears to be the norm. Transport Security Programs and emergency plans can be compact and effective, since many fewer interests are involved. And Airport Security Committee meetings can more readily be focused and purposeful.

92. Operators of the smaller airports indicated to the Review that the security problem which bothers them the most is simply feeling left out or left behind. They feel they need assistance, to understand the threats they might be facing, to do the risk-assessing needed to come up with the requisite strategies to

counter those dangers, and then to implement the moves they have decided upon or have had forced on them.

93. Recommendation IV above, which enhances the Security Analysis area in the DOTARS Office of Transport Security and has that area make available regular reports on aviation crime and terrorism, should help.

94. That help, offered so that airports will better understand the danger they face, will not be enough: they need to be better informed on what to do about it. The Office of Transport Security needs to establish a capacity dedicated to providing proper security-oriented training for those in the transport industry. That area should prepare clear instructions on the proper procedures for making security risk assessments guided by the Australian and New Zealand Standard for Risk Management and, either on its own or with working through appropriate consultants, stand ready to assist regional and smaller airports to evaluate their dangers and risks and to make suggestions on how those airports can best counter them. At the larger of the regional airports, and at the CTFR airports, ASIO's T4 should be called upon when appropriate to provide advice on physical infrastructure needs, but it needs to contextualize that advice in line with the Australian and New Zealand Standard for Risk Management. Cost should not be the determining factor in this risk assessment process provided all are objectively assessing the risk. However, Commonwealth funding assistance is desirable.

95. Still more will be required to draw regional and smaller airports into the national aviation security network as tightly as they should be. A periodic visit by the so-called 'Rapid Regional Deployment Team' demonstrating up-to-date methods for handling crisis situations will help. But what these airports need most is a menu of options for effective training on security related issues; from that, they can choose to address what they see as their shortcomings and weaknesses. Ideas already canvassed with the Review range from bomb recognition courses to engaging neighbouring communities in the defence of their airport. It will be incumbent on the area dedicated to training in the Office of Transport Security to consult with airports, initiate a professional survey and training needs analysis, and then proceed to help provide the training and assistance requested.

XV. It is recommended that the Office of Transport Security in the Department of Transport and Regional Services offer appropriate and increased security-oriented training and guidance and be in communication with airports, and especially regional and smaller airports, to survey and help discern their security needs. This role should include ensuring that ASIO T4 assistance with the design of physical security infrastructure is available where necessary or appropriate, with costs subsidised by the Commonwealth.

XVI Emerging technologies

96. Improvements in screening, detection, and monitoring equipment have been coming at an increasing pace. And with the demand for such improvements unlikely to fall away, the combination of accelerating technological progress and the workings of the marketplace will act to see still further advances come rapidly on line. But the speed with which new equipment and new methods are likely to appear, and the cost of acquiring them and implementing their use, will outstrip the ability of any single element in Australia's aviation security system to make informed decisions about what to acquire or to put in place.

97. Cutting through the competing claims of those marketing similar products, and testing the real as opposed to theoretical effectiveness of new technologies, should be the task of a designated official body. This body, in collaboration with leading aviation industry expertise could foster joint research, build up the knowledge in trialling advanced security equipment and methods, monitor the findings of relevant overseas agencies, and then assist the aviation industry to bring appropriate equipment online.

98. While the roles of the Commonwealth Security Equipment Committee chaired by ASIO's T4, the CSIRO, DSTO and others are important, enhancing the role (Annex 3) of the Science, Engineering and Technology unit in the Department of the Prime Minister and Cabinet appears to be the best current option.

XVI. It is recommended that a sufficiently resourced Commonwealth body, such as an enhanced role for the Science, Engineering and Technology Unit within the Department of the Prime Minister and Cabinet, be empowered to evaluate emerging technologies relevant to screening and other security-related efforts at airports and to recommend, oversee and assist the uptake of such technologies.

XVII Crisis management

99. Australia's systems for mitigating and handling threats from terrorism and criminality in the air and at airports are built on concepts of inclusiveness, consultation, and overlapping responsibilities. These are fine, as far as they go. But they do not go far enough, because they cannot substitute for direct lines of responsibility and control. Recognising the issue, ICAO Annex 17 Standard 3.2.4 requires the preparation and exercising of contingency plans for safeguarding against unlawful interference with aviation.

100. Particularly is this the case at times of crisis. As things stand, should a major terrorism-connected event occur at an Australian airport, complex consultation might still contribute to delays in implementing a response. The Review acknowledges the significant work undertaken in the various jurisdictions to develop incident response arrangements based on coordination, communication and consultation, but found little evidence that the exercising of these arrangements had adequately prepared all potential participants for the real-life, real-time circumstances in which those arrangements require implementation. If the 'incident response command and control arrangements' cannot be clarified by the adoption of a truly national model, as a fallback, the existing arrangements appear to require far more exercising with all the senior decision-makers involved.

101. In theory, the Australian Federal Police Protective Service, with its CTFR capability, would initially handle the problem. Then the local State or Territory Police would assume responsibility. Finally, should the dimensions of the event still loom large as a National Terrorist Situation, the Commonwealth could assume a strategic role.

102. But there is neither clarity nor simplicity around those shifts of responsibility. In a situation where damage and casualties from an attack at an airport are already high and more could well be in the offing, it is obvious that the first State Police constable arriving on the scene is not able to take control. But when, under what circumstances, and by whom the decision is made to turn the scene over to the local police is not clear. The position of Airport Police Commander provides an opportunity to improve and clarify existing arrangements.

103. The shift from State to Commonwealth responsibility may be problematic. Consultation and agreement between the two levels of government are called for. But between exactly whom in those Governments is not clear, nor is it clear what happens if

they are not in agreement. And if a National Terrorist Situation is to be declared, not only must the head of government in the affected State or Territory be consulted and agree, but the heads of government in the other States and Territories are potentially to be involved as well. The call-out of the Australian Defence Force can be equally daunting. This is all simply too messy and too contingent to be reliably effective at a time when lives will be at stake, uncertainty will be rampant, public concern will be high, and national and international media attention will be swelling.

104. As a first step, the incorporation of the role of the new Airport Police Commander in national plans and the practical exchange of some communications information and equipment between State and Territory Police and the policing force at airports would help. They would then be able to ascertain how to exchange control, once it was clear when that should happen.

105. Beyond this, Australia would do well to consider the use of a command structure such as the Gold, Silver, and Bronze system used in the United Kingdom which applies not only to police but to private industry and the voluntary sector (Annex 9). Frequent testing of this structure is what develops resilience of the type demonstrated in London after the 7 July 2005 bombings.

XVII. It is recommended that the arrangements for State or Territory Police to take over from airport AFPPS CTFR personnel in the event of a terrorist incident, along with arrangements for potential broader Commonwealth involvement, be reviewed and simplified by a senior Commonwealth/State working group under the supervision of the Secretaries' Committee on National Security. The changes should incorporate the role of the Airport Police Commander and ensure clear and consistent lines of responsibility, command, and control. The use of a command structure similar to the United Kingdom's 'Gold, Silver and Bronze' system should be adopted and include relevant industry and other non-government participants. Regular resilience exercises based on the new arrangements, which must be inclusive of all participants, should be held.

8. Conclusion

1. Airports and the aviation sector generally will continue to attract terrorists and criminals. Thus, the delivery of airport security and policing must be a continuing priority for Australia. This Review builds upon the Australian Government's developing framework by recommending further enhancements in terms of structure, systems and procedures.

2. It will always be the case, however, that changing threats and circumstances will mean that there is never a precise state of absolute safety and security and preparedness.

3. Consequently, the Review encapsulates three major themes in its recommendations which serve to promote proper security and policing, now and in the future, and they are:

   - information, in all of its forms, is a most valuable tool in confronting those who would violate the law and threaten order and security at airports; it must be shared rather than sequestered, used rather than filed away
   - organisation is crucial in and around airports, and in security and policing issues, this means that leadership and clear lines of responsibility are indispensable, as are effective partnerships and coordination among all stakeholders
   - ongoing training (including practical exercising) is vital for staff at all levels in all organisations both in their everyday work and in the event of an emergency.

4. The Review strongly agrees with the forward-looking conclusions of the Australian Government's 2004 'Protecting Australia Against Terrorism' document (Annex 3) that stated:

   "Planning for the future is a continuing long-term challenge and we cannot be complacent. The key principles underpinning the government's planning for the future are:

   - *intelligence assessments that are as comprehensive and accurate as possible about the nature and level of the threat we face;*
   - *sound risk management approaches that deliver the maximum level of security while making best use of the resources available to us;*
   - *a centrally directed approach to developing our arrangements and capabilities across the whole of government;*

- *effective partnerships with the states and territories and the private sector and continued engagement of the Australian public in the counter-terrorism effort; and*
- *closer international and regional cooperation in ways that complement and strengthen our domestic capacity to fight terrorism.*

…The Australian Government will continue to work closely with the states and territories and the private sector on a national approach to the protection of critical infrastructure. There will be an increasing focus on facilitating high-quality and targeted collaboration between Australian and international scientists and researchers on counter-terrorism technologies. If a terrorist incident has already occurred, then we must have well-practised national coordination arrangements for responding quickly and efficiently. What we cannot do is sit back and think the job is done."

5. This encapsulates the critical challenge ahead and it is to this end, to safeguard the people and lifestyle of Australia, that the recommendations of this Review are directed.

6. It will be necessary for recommendations made in this Review that are accepted by the Australian Government and COAG to be monitored during the course of implementation to ensure their effectiveness. Such monitoring should be undertaken by the National Security Committee of Cabinet on the advice of the Cabinet Implementation Unit in the Department of the Prime Minister and Cabinet, and should be done on a regular basis.

7. The Review believes that the fine tuning, further measures, and clearer roles it proposes will enable a balanced and achievable improvement to Australia's airport security and policing. However, further major gains will require a changed culture of cooperation, sharing, and openness to new technologies and methods across federal, state and private sector agencies and personnel, in order to replace the silos and insularity which continue to provide unnecessary weaknesses that could be exploited by criminals and terrorists.

Annexes

1. Review Submissions, Visits and Meetings
2. Australian Aviation Security Measures since 11 September 2001
3. *Protecting Australia Against Terrorism*, 2004
4. *Transnational Terrorism:* The Threat to Australia, 2004
5. Crime and Criminality at Australian Airports
6. Summary of NSW Police Submission
7. Comparative Police Numbers at Major Australian and Overseas Airports
8. The UK MATRA System
9. The UK Gold, Silver, and Bronze System and *Contest*
10. Singapore's National Security Strategy, 2004
11. Recommendations from the USA 9/11 Report, 2004
12. Cost of the Review
13. Biographies of Members and Secretariat Staff
14. Acronyms and Abbreviations

Annex 1

Review submissions, visits and meetings

On 7 June 2005, the Review was announced by the former Deputy Prime Minister and Minister for Transport and Regional Services the Hon John Anderson, the Attorney-General the Hon Philip Ruddock, and the Minister for Justice and Customs, Senator the Hon Christopher Ellison.

Advertisements seeking submissions were placed in major Australian newspapers on 17 and 18 June 2005 and 91 specific invitations were sent to relevant Commonwealth, State and Territory bodies as well as police and industry representatives.

The Review Team received 69 submissions from the general public, industry and government. In addition to the submissions received, the Review Team conducted a number of meetings and visited a number of airports:

Airports visited by the review team

Domestic airports

- Adelaide
- Alice Springs
- Avalon
- Brisbane
- Canberra
- Cairns
- Darwin
- Dubbo
- Gold Coast
- Hobart
- Horn Island
- Jandakot
- Melbourne
- Perth
- Sydney
- Townsville

International airports

- Changi, Singapore
- Chek Lap Kok, Hong Kong, China
- Gatwick, United Kingdom
- Heathrow, United Kingdom

- John F Kennedy, New York, United States of America
- Los Angeles International Airport, United States of America
- Meetings were also held in Canada with Transport Canada and Canadian Air Transport Security Authority (CATSA) in Ottawa.

Submissions received

1. Alan Jupp
   Affiliation: PlaneTorque Australia (Director)
2. David Carey
   Affiliation: Melbourne Aviation Society (Secretary)
3. Allan Leeson
   Affiliation: Burnie Airport Corporation (Chief Executive Officer)
4. David Stuart
   Affiliation: DFAT (First Assistant Secretary, International Security Division)
5. Paul Mullett
   Affiliation: Victoria Police Association (Secretary)
6. Jeff Lawrence
   Affiliation: Liquor, Hospitality and Miscellaneous Union (National Secretary)
7. John McArdle
   Affiliation: Adelaide and Parafield Airports (Manager Corporate Affairs)
8. Steve Whitmore
   Affiliation: Perth Airport (Aviation Security Manager)
9. Michael Vaughan
   Affiliation: Australian Federation of Airline Pilots
10. Maurie Tattle
    Affiliation: Toll Priority
11. Scott Work
    Affiliation: Cobham Flight Operations and Service (Manager Aviation Security)
12. Stephen Goodwin
    Affiliation: Brisbane Airport Corporation Ltd. (General Manager Operations)
13. Bruce Wernham
    Affiliation: Northern Territory Police (Deputy Commissioner)

14. Wayne Tucker
Affiliation: Hobart International Airport (Chief Executive Officer)

15. Rustom Kanga
Affiliation: iOmniscient (Chief Executive Officer)

16. John Nahyna
Affiliation: Australian Pacific Airports (General Manager Operations)

17. Bruce Kelton
Affiliation: Keltec Industries Pty Ltd (Director)

18. James Horne
Affiliation: Government of South Australia, Department for Transport, Energy and Infrastructure (Chief Executive)

19. Martin Engeler
Affiliation: Airline Tactical Solutions Pty Ltd. (Managing Director)

20. Karen Bishop
Affiliation: Attorney-General's Department (Security Law Branch)

21. Brad Geatches
Affiliation: Cairns Port Authority (Chief Executive Officer)

22. Paul Golland
Affiliation: Australian Federation of International Forwarders (Deputy Chairman and National Airfreight Director)

23. Derek Trafford
Affiliation: Regional Express

24. Andy Carroll
Affiliation: AQIS (National Manager)

25. Mark Burgess
Affiliation: Police Federation of Australia (Chief Executive Officer)

26. Simon Roberts
Affiliation: Tasmanian Government (State Security Unit)

27. Howard Ronaldson
Affiliation: Department of Infrastructure (Secretary)

28. Greg Gateley
Affiliation: Virgin Blue (Brisbane Security Manager)

29. Tony Negus
Affiliation: AFP (National Manager, Protection)

30. John Kilner
Affiliation: Department of Transport and Regional Services (Acting Executive Director of the Office of Transport Security)

31. Max Moore-Wilton, AC
Affiliation: Sydney Airport Corporation Limited (Chairman & Chief Executive)

32. Alistair Milroy
Affiliation: ACC (Chief Executive Officer)

33. Lionel Woodward
Affiliation: Australian Customs Service (Chief Executive Officer)

34. Ian McSweyn
Affiliation: ASIO (First Assistant Director-General, Security)

35. Danny Eatock
Affiliation: Gold Coast Airport ASC (Chairman)

36. Chris Bigg
Affiliation: Northern Territory Government (Executive Director Transport)

37. Ely Jensen
Affiliation: Australian & International Pilots Association (Legal Counsel Industrial Relations)

38. Christopher D. Corrigan
Affiliation: Patrick Corporation (Managing Director)

39. Geoffrey D Askew
Affiliation: Qantas Airways Limited (Head of Group Security)

40. Vincent McMahon
Affiliation: DIMIA (Executive Coordinator)

41. Warren Bennett
Affiliation: Board of Airline Representatives of Australia (Executive Director)

42. John Truman
Affiliation: Ballina Shire Council (Group Manager Civil Services)

43. John Green
Affiliation: NSW Police (Inspector)

44. Hon Dr. Geoff Gallop MLA
Affiliation: Western Australian Government and Police (State Premier)

45. Scott Work
Affiliation: National Jet Systems (Manager Aviation Security)

46. Hon Arch Bevis MP
Affiliation: Australian Labor Party (Federal Shadow Minster)

47. Terry Moran
Affiliation: Government of Victoria (Secretary Department of Premier and Cabinet)

48. Ken Keech
Affiliation: Australian Airports Association (Chief Executive Officer)

49. Jason Wood MP
Affiliation: Federal Member for La Trobe

50. Hon Peter Beattie MP
Affiliation: Queensland Government (Premier and Treasurer)

51. Hon Carl Scully MP
Affiliation: New South Wales Government (Minister for Police)

52. Andrew David
Affiliation: Virgin Blue Airlines Pty Ltd (COO)

53. Danni Whyte
Affiliation: Transport Workers' Union (Federal Policy Development Officer)

In addition to these, 16 private citizens provided submissions.

Scheduled meetings

The Review Team met with the following:

Ministers and Opposition

Federal

- The Hon John Howard, Prime Minister
- The Hon Kim Beazley, Leader of the Opposition with Hon Arch Bevis and Senator Kerry O'Brien
- The Hon Warren Truss, Minister for Transport and Regional Services

- The Hon Philip Ruddock, Attorney-General
- Senator the Hon Chris Ellison, Minister for Justice and Customs

State/Territory

- QLD Minister for Police & Corrective Services, The Hon Judy Spence MLA
- Victorian Minister for Police, The Hon Timothy Holding
- NSW Minister for Police, The Hon Carl Scully
- NSW Deputy Premier and Minister for Transport, The Hon John Watkins
- SA Deputy Premier and Minister for Police, The Hon Kevin Foley
- SA Minister for Transport, The Hon Patrick Conlon
- WA Minister for Planning & Infrastructure, The Hon Alannah MacTiernan MLA
- WA Parliamentary Secretary to the Premier, Ms. Margaret Quirk MLA
- NT Minister for Transport and Infrastructure, The Hon Chris Burns

Government bodies

Federal

- Department of Transport and Regional Services, Secretary Mr. Mike Taylor
- Inspector of Transport Security, Mr. Mick Palmer and staff
- Office of Transport Security, Executive Director Mr. Andrew Tongue and Acting Executive Director Mr. John Kilner and staff
- Department of the Prime Minister and Cabinet, Secretary Dr. Peter Shergold and Acting Deputy Secretary Mr. Duncan Lewis
- Attorney General's Department, Secretary Mr. Robert Cornall
- Protective Security Coordination Centre, Director Mr. Ed Tyrie and staff
- Customs, CEO Mr. Lionel Woodward and staff
- ASIO, Director-General Mr. Paul O'Sullivan and staff
- Australian Crime Commission, CEO Mr. Alistair Milroy

State

- Victorian Department of Infrastructure, Director Security & Emergency Management, Mr. David Harris
- Cairns Port Authority, CEO Mr. Brad Geatches and staff
- Horn Island, Airport Manager Mr. Buddy Ahmat
- Dubbo (NSW) City Council, Mr. Geoff Darby
- South Australia Department of Premier and Cabinet, Director of Security and Emergency Management Ms. Suzanne Carman
- Department of Defence Intelligence and Security, Assistant Director Joint Defence Facility Pine Gap Ranj Maharaj
- Dubbo (NSW) Police Superintendent, Mr. Stuart Smith

Police executive

- Australian Federal Police Commissioner, Mr. Mick Keelty, Deputy Commissioner Mr. John Lawler and staff
- Victorian Police Chief Commissioner, Ms. Christine Nixon and staff
- NSW Police Commissioner, Mr. Ken Moroney, Deputy Commissioner Mr. Andrew Scipioni and staff
- South Australia Commissioner of Police, Mr. Malcolm Hyde
- Western Australia Deputy Commissioner of Police, Mr. Tim Atherton
- Northern Territory Deputy Police Commissioner Mr. Bruce Wernham
- QLD Commissioner of Police Mr. Robert Atkinson and Deputy Commissioner Mr. Dick Conder
- Tasmanian Commissioner of Police Mr. Richard McCreadie and Deputy Commissioner Mr. Jack Johnson

Industry and associations

- Australia Post, Corporate Secretary Mr. Michael Mcloskey and staff
- Australian Airports Association, CEO Mr. Ken Keech, Chairman Mr. John McArdle, and Director Mr. Stephen Byron
- Canberra Airport, Managing Director Mr. Stephen Byron and staff
- Melbourne Airport, CEO Mr. Chris Barlow and staff
- Macquarie Airports Board, CEO Mr. Kerrie Mather and Chairman Mr. Richard Sheppard

- TNT, Mr. Brian Harding
- Qantas, Head of Group Security, Mr. Geoff Askew and staff
- Sydney Airport, CEO Mr. Max Moore Wilton and staff
- Toll IPEC, National Security Manager Mr. Rod Grimshaw
- Adelaide Airport Limited, CEO Mr. John McArdle and staff
- Townsville Airport, CEO Mr. Chris McHugh and staff
- Westralia Airports Corporation Pty Ltd, CEO Mr. Graham Muir and staff
- Avalon Airport, General Manager Mr. Tim Anderson
- Jetstar Airways, Mr. Phil Gregory
- Australian airExpress, Group General Manager Operations and International Mr. Wayne Dunne and staff
- Virgin Blue, Security Manager Mr. Phil Scanlon and Mr Greg Gately
- Hobart Airport, CEO Mr. Wayne Tucker and staff
- Alice Springs Airport, General Manager Mr. Dan McDonald
- Darwin Airport, CEO Mr. Ian Kew
- Jandacot Airport, General Manager Ms. Anne Watson and staff
- Northern Territory Airports Management, General Manager Mr. Don McDonald
- Brisbane Airport Corporation, General Manager Operations Mr. Stephen Goodwin and staff.

Airport Security Committee meetings attended

- Canberra Airport
- Melbourne Airport
- Sydney Airport
- Adelaide Airport
- Perth Airport
- Brisbane Airport
- Gold Coast Airport
- Darwin Airport.

Unions and associations

- Combined meeting at Australian Council of Trade Unions Headquarters, Convened by Mr. Richard Watts (ACTU) and including representatives from the Australian Licensed Aircraft Engineers Association, the Australian Manufacturing Workers Union, the Australian Services Union, the Electrical Trades

Union, the Liquor, Hospitality and Miscellaneous Union, the National Union of Workers, and the Transport Workers' Union

- Australian Federal Police Association, Mr. John Torr and staff
- Liquor, Hospitality and Miscellaneous Union, Union Representatives Mr Noel Witt and Mr Barry McKinnon.

Committees

- National Security Committee of Cabinet
- Joint Parliamentary Committee on Public Accounts and Audit
- Staff of relevant Australian Government Departments and Agencies attended five Advisory Committee meetings held on: Monday 20 June 2005, Wednesday 29 June 2005, Tuesday 19 July 2005, Friday 29 July 2005, and Friday 19 August 2005 to provide advice and assistance to the Review Team. Members included: Australian Customs Service; Australian Security Intelligence Organisation; Australian Quarantine and Inspection Service; Australian Crime Commission; Australian Federal Police; Department of Transport and Regional Services – Office of Transport Security and the Inspector of Transport Security; Department of the Prime Minister and Cabinet; Department of Foreign Affairs and Trade; Department of Immigration and Multicultural and Indigenous Affairs; and the Attorney-General's Department including the Protective Security Coordination Centre.

International meetings

United Kingdom

- Gatwick Airport, Sussex Police Airport Commander Chief Superintendent Mr. Phil Clarke
- Lewes Sussex, Chief Constable of Sussex Police Mr. Ken Jones
- Heathrow Airport, Airport Commander Chief Superintendent Mr. Jerry Saville
- Heathrow Airport, Metropolitan Police Mr. John Cox
- BAA PLC, Head of Security and Director for South East Asia Mr. Ian Hutchinson
- Officers from the Department of Transport
- Officers from the Home Office.

Additional meetings were held in:

Changi, Singapore; Chek Lap Kok, Hong Kong, China; John F Kennedy, USA; Los Angeles International Airport, USA; Transport Canada and CATSA in Ottawa, Canada.

Annex 2

Australian aviation security measures since 11 September 2001

The Review is grateful to the Department of Transport and Regional Services for providing the following information.

The *Aviation Transport Security Act 2004* and the *Aviation Transport Security Regulations 2005* came into effect on 10 March 2005. The main features of this new regime were:

- an increase in the number of regulated airports from 40 to 186 and of regulated airlines from 60 to 170;
- regulation of over 900 domestic cargo agents;
- greater controls over access to airports' secure areas;
- increased background checking requirements; and
- anti-theft measures to be applied to powered aircraft.

In addition, aviation industry participants are required to work with the Department of Transport and Regional Services to develop and implement operational Transport Security Programs (TSPs). The TSP is a preventative security program that sets out security measures and procedures to be implemented to safeguard against acts of unlawful interference with aviation. There are specific requirements for the TSPs of certain industry participants. These specific requirements are for security controlled airports, prescribed air service operators, airside facility operators and regulated air cargo agents.

Broken down by categories, the Australian Government has introduced the following measures since September 2001:

Legislative and Governance

- The *Air Navigation Act 1920* was amended in 2002 to update aviation security legislation.
- New aviation security legislation, the *Aviation Transport Security Act 2004* (ATSA) and *Aviation Transport Security Regulations 2005* (ATSR), commenced on 10 March 2005.
- The number of regulated airports was increased from 40 to 186 and the number of regulated airlines from 60 to approximately 170. There are also approximately 350 airport and airline approved TSPs, and many Regulated Air Cargo Agent (RACA) TSPs that are in the process of being approved.

- Establishment of Australian Government Agencies' Airport Security Committees (AGAASC) in major Australian international airports.
- The gradual upgrade of aviation security over four years at both Christmas Island Airport and Cocos (Keeling) Islands Airport.
- In December 2003, the Office of Transport Security was established in the Department of Transport and Regional Services and an Inspector of Transport Security was announced.

Security Identification

- The Aviation Security Identification Card (ASIC) regime was extended in December 2003 to cover all airports where passenger screening is required.
- Background checking of pilots was introduced from July 2004.
- From 1 January 2006, ASICs will be required by all aviation industry personnel with a legitimate reason to access landside and airside security zones at security controlled airports.
- All ASICs now have tamper-evident technology.

Freight/Cargo

- Trialling of new freight screening technology.
- Extension of regulatory regime for international air freight to domestic freight.
- Tighter controls over the carriage of domestic and international cargo including identification prior to sending internationally.

Aircraft

- Requirement for general aviation aircraft to have anti-theft measures including wheel locks or clamps, lockable controls, the aircraft being chained or padlocked to a permanent tie-down point, or the aircraft being inside a locked hangar.
- All airlines operating regular passenger transport aircraft with a seating capacity of 60 seats to be fitted with hardened cockpit doors by 2004, followed by extending this to aircraft with 30 seats or more, with the Government meeting the cost for aircraft with 30–59 seats.

Audit and Compliance

- The Australian Government has enhanced audit and compliance activities on aviation security. The focus is on timely and

effective industry compliance and identifying where and why breaches occur.

- Since the commencement of the *Aviation Transport Security Act and Regulations* on 10 March 2005 up to the end of June 2005, the OTS had undertaken:
- 60 security audits;
- 70 aviation security inspections;
- 46 Regulated Air Cargo Agent inspections;
- 50 systems tests;
- 350 visits to aviation industry participants; and
- 140 meetings with aviation industry participants about aviation security matters.

Under the Act, Aviation Security Inspectors are provided with a range of powers and responsibilities for the purpose of determining whether an aviation industry participant is complying with the Act and to investigate possible contraventions of the Act.

Screening

- Screening of passengers at some 39 airports with jet regular public transport services.
- The introduction of 100 per cent checked bag screening for all international flights by 31 December 2004, a year ahead of the International Civil Aviation Organization deadline.
- Capacity for domestic checked bag screening by 31 December 2004, with 100 percent screening of domestic checked baggage at all CTFR airports by July 2007.
- From 2002, extensive use of explosive trace detection at domestic and international passenger screening points.
- Threat Image Projection Systems for passenger x-ray screening equipment that randomly displays prohibited items or weapons on the screen to monitor the screening officer's attention and accuracy.
- New metal detection capability for about 146 regional airports.
- CCTV technology that will be trialled at several regional airports with 24/7 monitoring managed by the Office of Transport Security Operations Centre, with the potential for local police stations to receive live image feeds.

Security Presence

- Increased Australian Federal Police Protective Service presence at the 11 major airports providing Counter-Terrorism First Response capabilities (Sydney, Brisbane, Adelaide, Perth, Canberra, Melbourne, Alice Springs, Darwin, Cairns, Hobart, Gold Coast)
- Introduction of an in-flight Air Security Officer Program with armed officers on selected domestic services and international routes.
- Introduced the Australian Federal Police Protective Security Liaison Officer Network and the Australian Government Agencies' Airport Security Committees at major airports.
- Australian Federal Police Protective Service Regional Rapid Deployment Teams commenced operations in Victoria (visiting Mildura, Hamilton and Warnambool) in January 2005. Others are coming on line throughout 2005.

Training

- A joint training and exercise programme involving state, territory and federal police, which involves unique training on how best to respond to an aviation incident and include search, seizure, multi-jurisdictional counter-terrorism exercises, and crowd control at airports and in aircraft.
- Improved security training for regional airline and airport staff.
- Currently developing a security training and capability framework for employees in the aviation industry.

Annex 3

Protecting Australia against terrorism, 2004

In mid-2004, the Australian Government released *Protecting Australia Against Terrorism: Australia's National Counter-Terrorism Policy and Arrangements*. This report flows from the National Counter-Terrorism Plan launched on 11 June 2003. The following is a summary of that significant report.

The Prime Minister's foreword noted that the government has enhanced the roles of the National Security Committee of Cabinet and the National Counter-Terrorism Committee as the basis for a coordinated, whole-of-government approach to security matters and has committed over $3 billion since 2001, including to strengthen the counter-terrorism capabilities of intelligence agencies, the AFP and the ADF. The Prime Minister highlighted the goal of making it difficult for terrorists to plan, finance and carry out attacks and the need to engage the private sector and all Australians in the fight against terrorism. Other points in the 66-page publication of relevance to the Rt Hon Sir John Wheeler's Review are as follows.

The Government's three key counter-terrorism policy strategic objectives are: maximum preparedness, comprehensive prevention (including high-quality intelligence) and effective response. The Australian Government recognises that it is critical to our national security that it has cooperative relations with the states and territories, a strong partnership with the private sector in the protection of national critical infrastructure (eg in the transport sector) and broad engagement with the Australian public. Effective cooperation and coordination between the agencies of all government jurisdictions is equally important. As well as the traditional arms of national security, such as intelligence, diplomacy and defence, Australia's whole-of-government effort encompasses our law-enforcement, border-control, immigration, health and quarantine functions. The 2003 National Counter-Terrorism Plan created four levels of national counter-terrorism alert: Low, Medium, High and Extreme. Since 12 September 2001 the alert level has been Medium, defined as a medium risk of terrorist attack in Australia.

The states and territories have primary responsibility for funding and developing capabilities to respond to disasters, including terrorist incidents. State and territory police forces have operational responsibility in their jurisdiction for managing a terrorist incident. The Australian Government has a critical coordination role and specialist expertise to offer, should an incident exceed the capacities of a state or territory government. The Australian Government will consider, in consultation and agreement with any affected states or territories, whether a National Terrorist Situation should be declared. Such a declaration leads to the Australian Government taking an overall

responsibility for policy and broad strategy to resolve the situation. Australian Government counter-terrorism policy coordination is through the National Security Division of the Department of the Prime Minister and Cabinet, and operational coordination is through the Protective Security Coordination Centre (PSCC) in the Attorney-General's Department. Where appropriate, criminal investigations would be undertaken cooperatively, including through joint task forces. If the terrorist threat proves to be beyond the capacity of civilian authorities, the ADF can provide support under provisions of the Defence Aid to the Civil Community and Civil Authority in the Defence Force Act 1903. ADF counter-terrorism response capability has been significantly enhanced since 11 September 2001.

The Criminal Code (Section 100.1) defines a terrorist act as an action or threat of action that causes serious physical harm or death to a person, or endangers a person's life or involves serious risk to public health or safety, serious damage to property or serious interference with essential electronic systems. It is further defined as an action or threat of action intended to advance a political, ideological or religious cause, and to coerce or influence by intimidation an Australian or foreign government or intimidate the public or a section of the public. Key terrorist criminal offences are outlined in Part 5.3, Part 5.4 and Division 72 of the *Criminal Code Act 1995*. Other important legislation relevant to aviation security includes the ASIO Act, Customs Act, Migration Act, and the *Aviation Transport Security Act 2004* and 2005 regulations. The National Security Hotline commenced operations on 27 December 2002 to enable the confidential (and anonymous if sought) reporting of anything suspicious on 1800 123 400 or by email to hotline@nationalsecurity.gov.au 24 hours a day, seven days a week.

The Australian intelligence community (AIC) comprises ASIO, ASIS, ONA, DIO, DSD and DIGO. New powers became available to AFP and APS members in January 2004 to enable officers to work together more effectively in response to security incidents, particularly at airports. The Australian Crime Commission (ACC) was established in January 2003 to strengthen the fight against nationally significant crime. Terrorism is one of the highest national intelligence priorities set by the ACC. The Australian Transaction Reports and Analysis Centre (AUSTRAC) provides valuable intelligence from financial transactions to help protect Australia from the threat of money laundering, terrorist financing, people smuggling, drug trafficking and other major crime.

The Attorney-General's Department has primary responsibility for the development of critical infrastructure policy at the federal level. The Australian Government's approach has four main elements: taking the lead in identifying Australia's critical infrastructure and determining broad areas of risk; coordinating the development of strategies for mitigating risks to critical infrastructure; fostering

effective partnerships with state and territory governments and the private sector; and promoting domestic and international best practice in critical infrastructure protection. In conjunction with the states and territories, ASIO has constructed a database and a risk management methodology for identifying and prioritising our national critical infrastructure. Work on developing a strategic overview of risks to Australia's critical infrastructure will be an ongoing priority. There is a Trusted Information Sharing Network (TISN) coordinated by a Critical Infrastructure Advisory Council comprising key business leaders and relevant government agencies with a direct link to the National Counter-Terrorism Committee.

Since 11 September 2001 the government has strengthened our border security through six major initiatives: a tighter legal framework and increased enforcement powers for AFP, APS and Customs officials; enhanced immigration visa processing, information storage systems and airline liaison officer and overseas compliance networks; a greater capacity to detect fraudulent documentation and leading edge research into the use of biometrics to detect identity fraud; increased security in the screening of air freight and sea-borne cargo; increased cooperation between Australia and regional countries; and increased surveillance of the seas to the north and northwest of Australia. The Movements Alert List (MAL) has the principal electronic data on people and travel documents of concern to immigration, law enforcement and security authorities.

In December 2003 the Australian Government established the Office of Transport Security within the Department of Transport and Regional Services with principal responsibility for regulating aviation and maritime security. In April 2004, the Australian Government and all state and territory governments agreed to a National Transport Security Strategy to complement the National Counter-Terrorism Plan. The Australian Government also announced a new role of Inspector of Transport Security to investigate independently, when required by the Minister for Transport and Regional Services, a major security incident or a pattern or series of incidents that point to systematic weaknesses or the potential for failure of aviation or maritime regulatory systems. The focus of investigations is to be on learning, and the Inspector could have a land transport security reference if agreed with the relevant jurisdiction. Since 11 September 2001, the Government has strengthened the APS role at airports including with more explosives-detection dogs, expanded the aviation security regulatory regime, tightened airport access, increased passenger, baggage and cargo screening, required hardened cockpit doors, and improved security coordination among DOTARS, Customs, AQIS, AFP, ASIO and DIMIA at major airports.

The new Science, Engineering and Technology Unit located in the Department of the Prime Minister and Cabinet is helping to coordinate Australia's counter-terrorism research effort through links

with the private sector, universities and other government agencies such as the CSIRO and DSTO. Its four broad areas of priority are: chemical, biological, radiological and nuclear countermeasures; explosives; physical and information security; and intelligence, surveillance and operations.

Planning for the future is a continuing long-term challenge and we cannot be complacent. The key principles underpinning the government's planning for the future are:

- intelligence assessments that are as comprehensive and accurate as possible about the nature and level of the threat we face;
- sound risk management approaches that deliver the maximum level of security while making best use of the resources available to us;
- a centrally directed approach to developing our arrangements and capabilities across the whole of government;
- effective partnerships with the states and territories and the private sector and continued engagement of the Australian public in the counter-terrorism effort; and
- closer international and regional cooperation in ways that complement and strengthen our domestic capacity to fight terrorism.

In terms of the key role of intelligence, information sharing within the AIC itself, and between the AIC and the growing number of agencies involved in national counter-terrorism arrangements, will continue to strengthen. Australia's law-enforcement agencies will continue to increase their capacity to investigate and prevent terrorist activity.

The Australian Government will continue to work closely with the states and territories and the private sector on a national approach to the protection of critical infrastructure. There will be an increasing focus on facilitating high-quality and targeted collaboration between Australian and international scientists and researchers on counter-terrorism technologies. If a terrorist incident has already occurred, then we must have well-practised national coordination arrangements for responding quickly and efficiently. What we cannot do is sit back and think the job is done.

Annex 4

Transnational terrorism: the threat to Australia, 2004

In 2004, the Australian Government released a White Paper, *Transnational Terrorism: The Threat to Australia*, which complemented the Government's 2004 national security publication *Protecting Australia Against Terrorism*. Points of relevance in the 112-page publication to the Review by the Rt Hon Sir John Wheeler are summarised below.

Past terrorists often relied on state sponsors for capability beyond geographic borders. Today's transnational terrorists do not. Globalisation has made the financing of transnational terrorism easier, and international money-laundering to support terrorist operations is also easier. In addition to the use of front companies and non-government organisations, terrorism in South-East Asia (eg Jemaah Islamiyah, Abu Sayyaf Group) has been supported by other financial activities including fund-raising, extortion, kidnapping and ransom. Areas in Thailand and elsewhere are used to launder money and obtain forged identity documents. There are indications that terrorist funds are now also coming from drug trafficking.

Terrorists attack transport targets to inflict mass casualties and to target critical infrastructure so as to cause maximum damage and disruption to facilities and services vital to a nation's government and economy. Commercial aircraft are still a preferred target for terrorists seeking a high death toll. Good intelligence, better law enforcement, improved counter-terrorist legislation and tighter financial, transport and border protection and measures to protect critical infrastructure are central to Australia's broad-spectrum response to the dynamic, disproportionate and asymmetric risks of transnational terrorism. We must also face up to the threat of our own complacency.

Combating terrorism requires a larger number of government agencies and a wider range of functions than have normally been associated with national security. Our police, intelligence, security, customs, defence force, immigration and transport agencies, as well as our legal, development-cooperation and financial authorities all play important roles in supporting our international counter-terrorism effort. Coordinating the activities of these agencies is essential to achieving a whole-of-government approach to fighting terrorism. This is assisted by Australia's Ambassador for Counter-Terrorism and the new inter-agency International Counter-Terrorism Coordination Group. Key UN bodies involved in anti-terrorism are ICAO, the IMO and the UN Office on Drugs and Crime.

In dealing with the transnational threat of terrorism, the Government is committed to working closely with regional neighbours such as

Papua New Guinea and the Solomon Islands to strengthen governance and institutions and to reduce opportunities for exploitation by foreign criminal and terrorist elements. The AFP is helping a range of countries establish Transnational Crime Centres that strengthen their ability to investigate transnational crimes, including terrorism.

Disrupting the flow of funds to terrorists is a priority, and the Australian Transaction Reports and Analysis Centre (AUSTRAC) has a vital role in supporting global efforts to identify and halt the financing of terrorist-related activities. Australia is working with other APEC countries to tighten maritime and customs security and controls on the financing of terrorism. It is not possible to stop members of international terrorist groups from moving around, but effective border-protection measures can make it harder for them to do so. Intelligence is one of our best defences. The National Threat Assessment Centre (NTAC) is a dedicated 24-hour, seven-day-a-week operation that monitors, analyses, and assesses terrorist risks and threats. NTAC staff include ASIO, the AFP, ASIS, DIO, DFAT, DOTARS and ONA.

The majority of critical infrastructure is owned or controlled by the private sector or by state and territory governments, so a high level of cooperation involving all parties to protect this infrastructure is essential. Our ability to counter the terrorist threat will be most effective when the people of Australia and their governments work together. This means all Australians need to understand the nature of the threat and the actions these governments are taking to combat it.

Annex 5

Crime and criminality at Australian airports

The collection, the collation, and the interpretation of crime-related data from airports is far from complete. The Review fully supports the efforts now under way by the Australian Crime Commission and Australia's law enforcement agencies to improve this situation and to provide a fuller picture of criminality at the nation's airports.

Still, even preliminary generalisations and observations are useful, and at this stage the Review judges that some are feasible, at least as indicative statements, based on the data to hand. As noted on page 43, the data are seriously flawed by under-reporting and by a lack of police on-airport.

The great bulk of crimes reported at airports (Figure 5) are in categories which ordinarily would be handled by units involved in community policing:

- easily the single most reported crime is theft
- instances of theft range from single, opportunistic events, sometimes involving only minor items of little value, right up to organised, professional efforts involving ongoing systematic pilfering, even of highly valuable goods or equipment
- thefts occur both in the landside and in the airside areas of airports; at this point it is not possible to say which of these is more costly, or whether connections exist among perpetrators across the airside/landside divide;
- notable thefts at airports include theft of vehicles, usually from airport parking sites
- vehicles at airports also come frequently to notice as a result of their involvement in various road and traffic infringements.

Alcohol is an important factor:

- drink is probably a major influence in many of the instances of assault, criminal damage, and common breaches of the peace at airports
- a full accounting of this will prove particularly difficult, because it appears that in many instances trouble-makers under the influence of alcohol are handled in-house without reference to any recording authorities or are simply removed from the premises of the airport.

Though the outright number of drug-related offences appears to fall well below theft figures and probably below alcohol-induced crimes, illicit narcotics still stand out as the major concern at airports:

- basic drug-dealing and the use of drugs does occur at airports, but this appears to be a relatively small-scale issue
- the major problem is the importation and transit through airports of shipments of illicit narcotics bound ultimately for delivery off-airport
- with screening for drugs of passengers, baggage and cargo done only on arriving international flights, and not on domestic flights nor on those departing internationally, the full dimensions of the problem remain unclear;
- cannabis is moved through airports, but its importance does not rival that of heroin, cocaine, or amphetamine-based drugs
- a particular worry will prove to be the high number of professional criminal organisations with international connections
- because of the substantial sums of money involved, it will probably turn out to be drug-related criminals who are most responsible for subverting or suborning airline and airport employees.

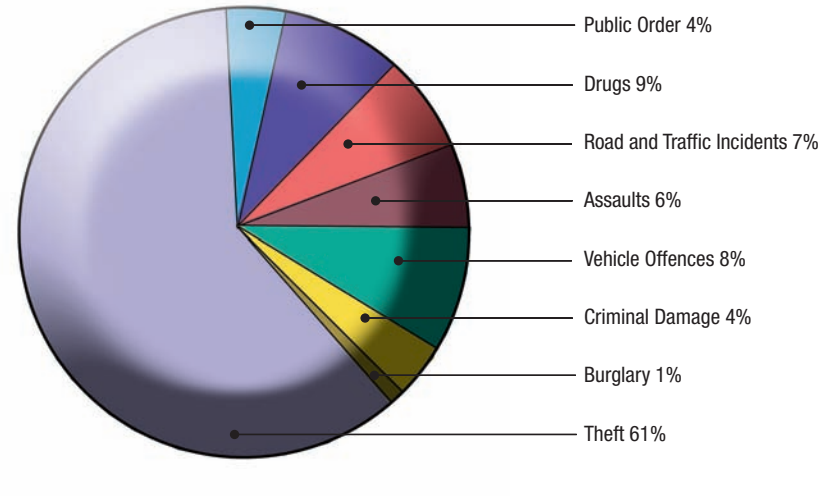
The attention of law-enforcement officers on the ground at airports will continue to be diverted to offences which occurred in mid-air:

- incidents of abusive or threatening behaviour aboard flights appear to have occurred at an average of about two per day over the past five years, and these demand action once an aircraft has landed
- hoaxes and bomb-threats, including by notes, occur aboard flights as well as on the ground, and such flight-specific incidents as smoking aboard an aircraft or using a mobile telephone counter to instructions also happen; these also require the attention of police units after the aircraft has set down.

As a rule, the bigger and busier an airport, and the more significant its international connections, the greater the likelihood of its having a larger and more deeply entrenched problem with crime:

- Sydney stands out in almost every category, followed by Melbourne
- the smaller CTFR airports with no international flights, Hobart and Canberra, are much less at risk.

FIGURE 5:
Criminal activity at all Airports (2000 – 2005 data)



Annex 6

Summary of NSW Police Submission

A NSW Police Submission formally submitted to the Review by Police Minister Scully on 26 August very powerfully makes the case for the significant risk of serious criminality at major airports and provides a number of domestic and international examples. A strong case is also made for the need for a much larger and integrated police presence at Sydney Airport including a joint multi-agency intelligence cell. Key extracts from the submission are reprinted below.

NSW Police and others have previously reviewed policing and security arrangements at Sydney Airport and made recommendations for change on the basis of the identified concerns. These deficiencies are usually caused through multiple security and policing agencies having authority over separate functions and areas of the airport, with resultant gaps in security processes exposing avenues for criminal activity and risks to safety. Anecdotally, these problems are mirrored at airports throughout the country.

The fragmented security systems highlighted in the late 1990s exposed Sydney Airport's vulnerability to criminal activity. The lack of inter-agency integration has resulted in gaps in security that provide opportunity for criminal activity by airside staff. More recently (2004–2005) this issue has come under scrutiny by media and government, culminating in the Federal Government commissioning a review of airport issues.

NSW Police advocates an integrated security environment where risks are assessed, and all threats to security are managed in a cohesive fashion. (For) the investigation of organised or serious crime and matters that cross agency boundaries, a multi-jurisdictional task force, the Joint Airport Crime Unit is proposed.

The policing requirements at Sydney Airport can be categorised into four areas:

- Community policing - inclusive of reactive/proactive intelligence based response.
- Criminal investigations (including serious and organised crime).
- Emergency and Security Incident preparation and management.
- Public Order Management – Crowd control during official visits etc.

Recent comment has been made likening Sydney Airport to a major shopping centre connected to a transport system. It has been suggested that the State policing response is commensurate with that comparison. Sydney Airport does contain large areas of shopping

space and, consequentially, a component of criminal activity at Sydney Airport is retail thefts. However, there are wider considerations that negate this argument. Shopping centres do not have 26 million passengers annually travelling through them via 266,746 aircraft movements, nor do they have over 45,000 employees requiring varying levels of security authorisation including National and International probity.

The needs of an Airport the size and importance of Sydney require more than a standard 'community policing' response. Community policing alone, consisting of pro-active and re-active policing, does not cross the airside/landside barrier; does not address baggage tampering and theft, criminal records of employees, transportation of drugs within the airport environment, or the deterrence of and immediate response to terrorist threats. Similarly, the provision of Counter Terrorist First Response (CTFR) services, a uniformed continuously patrolling security force designed to deter and/or respond to politically motivated violence, does not address the wider policing and security risk setting. Risk assessments have identified that politically motivated violence is not the major crime category most likely to occur at Sydney Airport. Intelligence analyses have revealed that the greater risk is from smaller criminal incidents and the relaxation of security standards and/or a breakdown in the effectiveness of organisational systems and processes thereby leaving airport safety compromised.

Policing and security strategies for Sydney Airport rely on Federal and State Police co-ordination of functions from within silos, with representatives meeting sporadically to exchange dated information, rather than timely intelligence. A better model is an operationalised, integrated approach that was successfully used during the Sydney Olympics (2000). The level of interagency integration and co-ordination involved more than coming together for meetings and exercises. Intelligence was shared across law enforcement agencies immediately it was received and assessed, joint activities were conducted and strategies were developed to share resources effectively, regardless of which organisation they were drawn from.

Essentially this submission identifies an opportunity to dissolve bureaucratic processes and perceived jurisdictional boundaries that have hindered serious and organised crime investigations at airports, and integrate policing and security organisations and processes. Specifically, this document recommends:

1. That NSW Police provide an enhanced policing service to Sydney Airport through one of three proposed models.
2. That a Joint Airport Crime Unit encompassing a joint intelligence cell consisting of NSW Police, Australian Federal Police, Customs and Immigration be established to collect and disseminate relevant intelligence relating to crime at Sydney Airport.

3. The a Joint Airport Crime Unit refer matters directly to the NSW Police State Crime Command using existing guidelines for the investigation of serious and organised crime within NSW airports that fall within the charter of that command, or similarly refer matters to the appropriate agency for investigation.

The history of policing at Sydney Airport is summarised below:

- In 1970, the strength at the Airport Police Station was seven (7) sworn officers, with the majority of offences dealt with under Commonwealth legislation.
- In 1991 the Australian Federal Police (AFP) withdrew its uniformed presence outside of Australian Capital Territory. Federal legislation was passed conferring powers upon APS officers and until 1993, where APS officers were Special Constables in the State of NSW.
- During 1991–1997, the Airport Police Sector was staffed by: three (3) sergeants and twenty two (22) constables. These officers primarily performed beat duties and VIP protection in support of the head station, Mascot. These officers were located at the Airport Police Station, situated close to the Domestic Terminals.
- In 1997, NSW Police undertook a re-structure that saw the formation of 80 Local Area Commands (LACs) across the State as centres for service delivery. Botany Bay LAC was established as an amalgamation of the Mascot and Malabar Patrols.
- In 2002, police and the 'Sky Marshalls' jointly occupied the Airport Police Station. However in 2005 police related infrastructure was removed from that facility.
- To date, deployments to Sydney Airport occur via calls for service, or high visibility policing (HVP) patrols. Figures obtained indicate HVP is conducted on average twice per day per terminal.

Any consideration of the policing needs should encompass the issue of an Airport Precinct as a defined area for the purpose of comprehensive policing services.

CTFR was established to ensure compliance with the Commonwealth responsibilities under the terms of Annex 17 to the International Civil Aviation Organization (ICAO), when the Australian Federal Police withdrew its presence at airports as a uniformed entity in 1991. CTFR is defined in the *Aviation Transport Security Act 2004*, Aviation Transport Security Regulations 2005, and Sydney Airport Security Program as a 'response capability that provides a uniformed, armed initial response to acts of terrorism involving airports and other unlawful interference involving aviation'. It now also encompasses the

provision of preventative measures to deter acts of terrorism. CTFR functions both as a 'visible deterrent' to potential acts of interference and a response framework to actual occurrences of interference to aviation. In accordance with the prescriptive requirements of the Regulations, CTFR is undertaken by members of a contracted organisation from the AFPPS or police from the relevant State.

The AFPPS (formerly Australian Protective Service) at Sydney Airport has a strength of approximately one hundred and twenty (120) personnel. Twenty (20) personnel per shift are deployed during airport operations, with four (4) additional officers per shift paid for by the Commonwealth Government. To a lay-person or visitor from another country or State, AFPPS are seen as members of the police. However, Protective Service officers have neither the capacity, knowledge or legislative power to take necessary action should they detect or be made aware of a breach of laws or be asked to take reports of incidents. The only power of arrest conferred on these officers is in relation to 'protective service offences', and in those situations they are required to detain and immediately contact the relevant police force and hand that person to them.

1. The current policing of Sydney Airport is fragmented.
2. Recent changes to aviation security legislation including the Aviation Transport Security Act 2004 have given NSW Police as designated Law Enforcement Officers (LEOs) a much greater capacity to traverse the airport precinct. However NSW Police does not have the resources, human or financial to support an increased role.
3. Counter-Terrorist First Response as an exclusive deployment strategy may not be the most effective means of providing policing response at the Airport.
4. Subtle changes to Sydney Airport as a result of the world security environments since 1999 have seen some improvements to management and coordination and a greater focus on security. This has not spread to an integration of operational strategies and policing practices to address the multi-jurisdictional nature of the airport.

Australia can no longer rely on that fact that it has enjoyed a relatively incident free aviation record, both in safety and crime. There is global consensus that airports are infiltrated by organised criminals, and are susceptible to terrorist activity and criminal networks. Not all organised crime is terrorism, but all terrorism is organised or has organised crime as its foundation. Furthermore the mere presence of organised criminals adds to the general vulnerability of airport security. Consequently there is a need to address elements of organised crime in future airport security practices and procedures.

Much attention is given to passenger movements; less has been paid to the global problem of organised crime and cargo. The anomaly is that whilst all individual passengers are scanned at airports, luggage in airplane holds receives less attention.

Addressing serious and organised crime at international airports has always been fundamentally problematic for the following reasons:

- The lack of tangible statistical evidence indicating organised crime exists.
- The reluctance of stakeholders to highlight that evidence due to fiscal concerns.
- Ambiguous reporting procedures resulting in information silos.
- Bureaucratic barriers to the release of stakeholder information and intelligence.
- Strong commercial interests and pressures.
- Crime ownership.
- Privacy legislation.
- Unreported or underreported crime.

One of the issues for law enforcement agencies justifying an airport response is that global serious and organised crime may not always occur within the airport but is inextricably linked by its relationship to:

- Airport staff
- Cargo movement
- Drug trafficking
- Immigration breaches
- The facilitation of children and sex workers from South East Asia
- Flight of wanted persons for indictable offences.
- Major disruptions to the operations of Sydney Airport, from criminal actions
- Critical incidents that arise as a result of criminal negligence or complacency.
- Threats of politically motivated violence.
- Passport and Ticket fraud.

The technology and information gathering processes at airports can facilitate a significant range of information on known criminals. Advances law enforcement agencies have made in facial recognition,

vehicle recognition and passport fraud have also highlighted what types of criminals are arriving and departing New South Wales domestically and internationally. However, the amount of evidence being held in law enforcement silos is most usually apparent only after those agencies conduct a joint investigation. The information collected across the stakeholders can provide major crime investigators with a range of intelligence on suspects.

NSW Police proposes a Joint Airport Crime Unit. Under this model intelligence is collected from a multitude of sources, shared and disseminated quickly to investigators and relevant agencies. It also provides investigators with the means of requesting information prior to the movement of the suspect with 'tagging' of passengers available through stakeholder agreement.

The following are examples of organised crime activity reported through intelligence channels as occurring on or near Sydney Airport [16 examples were provided, eg $1m theft of mobile phones in 2001]. A perusal of operational orders maintained at Botany Bay Local Area Command identified that 33 per cent of recorded operations in 2005 related to Sydney Airport.

An analysis of local investigations involving Sydney Airport has identified that since the 2000 Olympics, the LAC has investigated:

- Deceased persons landed at the Airport.
- Ticket Fraud.
- Robbery offences both landside and airside.
- Internal theft.
- Organised internal corruption
- Extortion attempts on airlines.
- Organised criminal gangs working in the airport – fraudulent rental of cars.
- Organised criminal gangs working in the airport – tourist luggage theft.

The AFP currently assess and check persons requesting ASIC clearance. The global trend is a tightening of this access.

Based on the British experience, it is not unreasonable to assume that organised criminals can infiltrate and commit offences at Sydney Airport.

The most recognizable 'serious and organised crime' associated with airports is that of drug smuggling or trafficking. Drug trafficking is inextricably linked to organised crime.

Historically there have been coordination problems with drug investigations as the AFP, Customs, National Crime Authority (now Australian Crime Commission), NSW Crime Commission, ASIO, and all other State and Territory Police agencies have all had cause to conduct their own separate drug and organised crime investigations at Sydney Airport. The proposed Joint Airport Crime Unit would address this issue. Where there are multi-agency responsibilities for various safety and security risks, it is possible for real and perceptual demarcations to arise. This situation can result in agencies becoming isolated from each other in terms of operational focus, information management and decision-making.

As noted previously, the risk of compromise to security at Sydney Airport is greater from criminal activity than from politically motivated acts of terrorism. There is an identifiable overseas trend towards major crime incidents taking place landside and airside within airport precincts. The criminal activity includes stolen cargo, illegal immigration, gun trafficking, theft, armed robbery and extortion. Of importance to the general operational safety and security of Sydney Airport is therefore the relationship between the deployment of security resources and the management of other policing responsibilities. NSW Police's integrated response model will also allow action to be taken to address identified risk behaviour on the part of employees.

A potential weakness in organisational procedures is to become complacent in a 'secure' environment. Where commitment to general safety and security measures may be lacking, the coordinated security and policing model provides greater opportunity for early identification of the problem. Visible policing also acts as a deterrent to criminal activity. A series of Memorandums of Understanding clearly defining the roles, functions and co-ordination responsibilities would be developed between NSW Police, the Airport Operator and all relevant stakeholders. This will ensure lifting of demarcated airside / landside barriers and integrate the community policing activity with existing security arrangements.

It is the NSW Police position that full funding should be provided for the provision of facilities, resources and dedicated policing services in accordance with the three models outlined. Attachments to this document outline an indicative model of the costs that would reasonably expected to be incurred per annum in providing 52, 100 or 150 police in those models. This includes full costs associated with personnel, vehicles, radios, uniforms and appointments. These costs are additional to the current authorised policing strength and primarily dedicated to Sydney Airport therefore unavailable for general policing.

Currently, NSW Police attached to Botany Bay Local Area Command use the standard NSW Police channel whilst at Sydney Airport. It is

anticipated that should an Airport Police Precinct be established, policing and relevant law enforcement agencies will work on the same channel, operating from the Sydney Airport Terminal Operations Centre with access to extensive CCTV systems of the airport.

Complementary to any of the above models for policing at Sydney Airport is the establishment of the Joint Airport Crime Unit to focus on serious and organised crime. This multifunctional unit would comprise the four key aviation law enforcement stakeholders: New South Wales Police, Australian Federal Police, Australian Federal Police Protection Service, Customs/Immigration. Current liaison arrangements would remain with the following agencies:

- Australian Crime Commission
- New South Wales Crime Commission
- ASIO
- Department of Foreign Affairs & Trade
- Department of Immigration and Multicultural and Indigenous Affairs
- Australian Quarantine and Inspection Service
- Private stakeholder security companies
- Corporate Aviation entities.

Aligned to the British MATRA (Multi Agency Threat and Risk Assessment Model) each stakeholder would contribute to the Joint Airport Crime Unit by providing intelligence and resources to combat major threats of serious and organised crime within the airport precinct in a consistent and managed framework. Central to this coordinated approach is the Intelligence Cell. This provides a single location where all stakeholder holdings of information on passengers, cargo, movements, air ground staff, flight crews and airport staff can be collected and assessed. Police acknowledge that the airport operator as well as aviation industry organisations are an essential component within this model, whereas current laws and requirements restrict the level of information that may be provided to non-law enforcement bodies.

The policing and security requirements of Sydney Airport require innovative strategies to manage a diverse working environment where State and Federal legislation and agencies overlap. The truth is, no one body is currently responsible for all of these functions on airport.

NSW Police submits that the most appropriate and cost effective method of providing a secure airport environment requires the following elements:

- An integrated multi-agency approach to the gathering and dissemination of airport intelligence;
- A multi-agency system of assessing and investigating serious and organised crime; and
- The provision of funded dedicated proactive and reactive policing of the airport working in collaboration with other airport policing and security forces.

To date, the work involved in preparing this submission has been undertaken by NSW Police in relative isolation. There is limited advantage in developing any valid proposal further without engaging the relevant airport stakeholders, including other policing and security agencies. Not to involve these agencies in the development of the most appropriate policing and security management system would perpetuate these identified deficiencies, leaving Sydney Airport vulnerable not only to the incidence of crime and terrorist threat, but to the perception of vulnerability.

Annex 7

Comparative Police numbers at major Australian and overseas airports

Table 1:
Australian airports

Station	Passenger numbers 2004	Permanent Police Presence Jurisdiction + CTFR
Adelaide	4,966,321	0+27
Alice Springs	609,676	0+16
Brisbane	14,059,998	0+61
Cairns	3,550,000	0+29
Canberra	2,437,160	0+25
Darwin	1,182,000	0+20
Gold Coast	2,576,940	0+15
Hobart	1,380,849	0+16
Melbourne	19,160,000	2+56
Perth	6,038,804	0+51
Sydney	26,425,640	0+110

Note: *Counter-Terrorism First response (CTFR) numbers include PSLO and AFPPS CTFR.*

Table 2:
Overseas airports

Station	Passenger numbers 2004	Permanent Police Presence Jurisdiction + CTFR
Hong Kong	36,711,920	400
New York JFK	37,518,143	400
Los Angeles LAX	60,688,609	400
Singapore	30,353,565	520
Manila	12,917,000	855
Frankfurt	51,098,271	1804

Notes: *Passenger numbers except Manila from Airports Councils International.*

Hong Kong Police numbers include the Aviation Security Unit (Rapid Response complement).

J.F. Kennedy Police Officers are trained in multi-tasking such as fire fighting, aircraft crash and aircraft emergency response.

Singapore Police numbers include SATS (Singapore Airlines Terminal Service Police) and AETOS (formerly Changi Police) and special investigators.

Manila passenger numbers are for 2003.

Police numbers include the Philippines National Police, Aviation Security Group (ASG) 271 officers; ASG Headquarters coordination, 75 officers, Special Operations & Weapons Unit, 76; Manila International Airport. Authority Police, 425 officers; and the National Bureau of Investigation (NBI), 8 officers.

Frankfurt has two types of police forces at the airport – both are armed and uniformed. One force (around 110 officers) is provided by Hessen (Federal State) to police public safety, crime prevention and patrol the take off and landing flight routes outside the perimeter fence. The other is the Federal Police (Bundespolizei – around 1694 officers) who look after (Passport) control and Aviation Security. It was not possible to obtain data excluding passport control which could have almost doubled the police numbers.

Annex 8

The UK MATRA system

Following advice from a 2002 inquiry into airport security headed by the Rt Hon Sir John Wheeler, the United Kingdom has introduced and maintained a new system for boosting security at airports, called the MATRA, because it is centred on creating and regularly updating formal documents called Multi-Agency Threat and Risk Assessments.

The MATRA System was developed jointly by the Department for Transport, which is responsible for aviation security, and the Home Office, responsible for counter-terrorism policy. The two Departments set up MATRA trials at five UK airports: Heathrow, Birmingham, East Midlands, Newcastle and Glasgow. When the System proved its worth, it was taken up as a national model.

Producing a MATRA involves four main phases:

- Threat Assessment: identifying the types of threat, the likelihood of each of these threats occurring, and the possible impact on the airport
- Vulnerability Assessment: determining what the key assets are and how they can be exploited, then examining the mitigating controls in place and their effectiveness, and considering possible remaining weaknesses
- Risk Assessment: making an assessment of the probability of an attempt and the likelihood it may succeed, thus determining the residual risk
- Risk Management: developing action plans to address weaknesses and mitigate identified residual risks.

The MATRA system is designed to produce an accurate assessment of the threats to individual airports from crime and terrorism; to identify any gaps and overlap in existing security regimes; and to develop plans for the management of risks. The work of thinking through the issues and producing the document is done by a group of airport security stakeholders: uniformed police, industry operators, government agencies, aviation-security inspectors, and any others with serious interests. The model is not a one-size-fits-all approach but rather is designed for each MATRA group to scale down the process according to local circumstances. And the aim is for members to adopt a security plan which is jointly owned and which can be routinely revisited and altered depending on developments.

The model encourages a culture of cooperation through sharing information, meetings, strong leadership, and linkages with other airport committees (where MATRA groups are meant to be strategic, other groups tend to be operational). It is, in short, an all-way communication process.

MATRA risk assessments are considered in an international, national and local context. If, for example, there are key dependencies beyond the airport perimeter that need consideration, such as transport infrastructure, communications systems, navigational aids, utilities and fuel, they will be considered as well.

In the UK, a MATRA Secretariat has been established to support members in setting up their groups. The Secretariat is made up of representatives from the Home Office and the Department for Transport. MATRA groups are required to report regularly to the Secretariat and lodge risk registers with them once complete.

A UK National Aviation Security Sub-Committee was also established at around this time. Its tasks include coordinating national-level control-authority input to MATRAs; collating and comparing airport crime and incident data; monitoring MATRA progress at individual airports; and promulgating advice to MATRA-producing groups on new developments needing consistent treatment across all airports.

(It should be noted that the terms and methods cited are those of the UK MATRA System. They are not necessarily the same as those employed by Australian agencies or in the Australia/New Zealand Standard AS/NZS 4360:2004.)

Annex 9

The UK Gold, Silver and Bronze system and *Contest*

Admiration has been widely and often expressed for the way in which London handled the July 2005 bombings. The police, the transit authorities, the emergency services, the hospitals, and the private sector put in splendid separate but coordinated efforts. The population also reacted in a positive fashion, were helpful to the authorities and determined to carry on with their lives.

Many factors contributed to the way in which those charged with sudden responsibilities slipped easily into them and to the resilience shown by Londoners and London's institutions. But key elements underlying the successful performance were two models of organisation and action already in place and well-drilled: the Gold, Silver, Bronze model of a command structure for the uniformed authorities, and a strategy for the struggle against terrorism, called *Contest*.

Gold, Silver, Bronze

This model of a command structure serves as the basis for UK Police Service preparations for contingencies such as major incidents, demonstrations and large sporting events. It is used to address the consequences of all unforeseen events, including terrorist attacks.

The model has three specific command-function levels: Gold addresses strategic matters; Silver, tactical; and Bronze, operational. Commanders at each level have support teams to assist them in their roles.

Use of these generic terms allows for an understanding and coordination of relationships and interdependencies across government agencies and between government and the private sector. The model allows for heightened clarity of roles and responsibilities across and between different organisations and with business.

The **Gold Commander** is the officer in overall command. He or she has responsibility and accountability for handling the incident or event, and chairs a strategic co-ordinating group should an incident demand a multi-agency response. The mission is to set, review, and update the strategy, and not to become involved in tactical decisions. So, for instance, he or she decides the size of the force needed to contain or control the event, but the decisions on which forces to deploy where, or what specifically they are to do once they are in place, rest with officers below in the structure. The Gold Commander does, however, approve such tactical plans to ensure they coincide with his or her strategic intentions.

The **Silver Commander** is responsible for developing and coordinating the tactical plan, and for seeing that it is congruent with

achieving the strategic intention of the Gold Commander. He or she also is the important link in the command chain between the Gold Commander and the Bronze Commander(s) actually in charge of forces on the ground, part of his or her function being to ensure that everyone is informed about continuing developments. The Silver Commander is also responsible for ensuring that the actions to be employed by Bronze Commanders meet the strategic intentions of the Gold Commander and are consonant with his or her own tactical plan.

Each **Bronze Commander** is responsible for the implementation of the Silver Commander's plan by the use of appropriate action and deployment within his or her geographical or functional area of responsibility. The Bronze Commander must fully brief their staff on the bigger picture, and keep the Silver Commander updated on current developments, including any variation from agreed tactics forced by developments on the ground.

Successful application of the model depends upon:

- the highest authorities being aware of the capabilities of their subordinates and choosing the right people to become the Gold and Silver Commanders to handle the event
- once those Commanders are in place, leaving them to get on with the job, free of interference from outsiders regardless of their rank
- giving to the Gold Commander the power to assess the situation and prioritise when competing demands arise on available resources
- ensuring that constant communication between levels is maintained, including regular give-and-take briefings, so that each knows who is responsible for achieving each objective, who is responsible for minimising each risk identified, and who is in direct control of each of the available resources
- quickly putting in place protocols regarding intelligence dissemination which enables Commanders at all levels to have immediate access to relevant information, including that from debriefings on the spot
- recording every decision taken by Commanders, so that post-event analysis can assist in improving future performance
- regular discussion exercising to clarify and validate roles and responsibilities, and identify deficiencies in security policy and planning.

Importantly, though the Gold, Silver, Bronze structure is a police-command model, it has been mirrored by professional, non-government, and charity organisations, from the Red Cross to chaplains. It is also understood and to some degree emulated by industry and business.

Contest

Contest is an overall counter-terrorism strategy, with a straightforward aim: to reduce the risk from International Terrorism so that people can go about their business freely and with confidence. It has four inter-linked elements which contribute to reducing that risk:

- prevention: attempting to understand and address the root causes of terrorism
- pursuit: going after terrorists, and those who support them, before they strike
- protection: strengthening all defences against potential attacks
- preparation: being ready to handle and to minimise the consequences, should an attack occur.

While prevention and pursuit are essential elements in the overall strategy, it was facets of the protection and preparation elements which were notably helpful in enabling London and Londoners to do so well in the period immediately after the July 2005 bombings. Key among them are:

- drawing the entire community, including Muslim communities, into an effective relationship with the authorities, fostering a sense of trust and shared responsibilities, and resulting in an easier flow of information among all concerned
- establishing an effective partnership between government and the business community, enabling the latter to gain confidence that the authorities recognise the importance of business activities, that confidential information can and will be shared in either direction and will be treated with sensitivity, and that requests for assistance will be acted upon quickly and in a professional manner
- planning for the involvement of emergency-service units; hospitals and medical professionals; chaplains, family-liaison officers, and counsellors; and even coroners and morgue attendants
- looking to use all of these to gather information to understand what transpired and how to move ahead
- putting in place the frequent exercising and training regimes which enable the strategy to work under pressure.

Contest is defined by two unambiguous objectives, to ensure all government and private sector activity is:

- creating an environment hostile to terrorists' preparation and planning; and
- focused on identifying and resolving suspicious activity.

Annex 10

Singapore's National Security Strategy, 2004

Last year, Dr Tony Tan Keng Yam, Singapore's Deputy Prime Minister and Coordinating Minister for Security and Defence, publicly released Singapore's National Security Strategy 'The Fight Against Terror'. A number of themes in the document are relevant to those emphasised by the Review by the Rt Hon Sir John Wheeler DL.

In his August 2004 preface, Deputy Prime Minister Tony Tan urged that the key ideas behind this strategy *'be disseminated widely to create awareness and enlist support. Transnational terrorism is not a passing menace. It is a long-term peril. The cornerstone of Singapore's strategy is a stronger and more robust inter-agency network. A stove-piped approach to internal security and external defence will no longer work. At its core, our national security strategy should aim to enhance coordination among the different ministries and national security agencies in Singapore. We need, furthermore, to strengthen our national resilience.'*

The Fight Against Terror: Singapore's National Security Strategy includes the following.

We cannot guard every installation or scan every visitor. What we can do is reduce the threat to a tolerable level, so that terrorism does not have a significant impact on our society and economy. We formed new agencies such as the Homefront Security Office and the Joint Counter-Terrorism Centre, while also reinvigorating existing units such as the National Security Secretariat.

The strategy outlines the nature of the threat that confronts Singapore today, briefly explains Singapore's security priorities, and describes the strategy we will adopt to counter terrorism. It seeks to provide all Singaporeans with a sense of where we are now, where we must go and what we must do in this security landscape.

Singapore's national security strategy aims, principally, to prevent threats to national security from developing in the first instance; protect Singapore against the more likely threats; respond to such threats if prevention and protection should fail; and achieve a quick recovery to return Singapore to a state of normalcy.

We intend to achieve these aims through tighter networking and inter-agency coordination. Terrorism is a problem that cuts through governmental divides. We must ensure that our coordination in the lead-up to crisis situation falls into place as a matter of routine. We have taken a key step by establishing a National Security Coordination Secretariat at the Prime Minister's Office, right at the heart of government.

Osama bin Laden's Al-Qaeda has explicit global aims. It seeks to destroy the United States and its Western allies and establish pan-Islamic caliphates, overturning the international political order. Jemaah Islamiyah, a movement inspired by a similar vision for the world, is its principal South-east Asian representative. Bombing continues to be the favoured tactic among terrorists, including those from Al-Qaeda and Jemaah Islamiyah. Attacks are often aimed at defenceless civilians, with little regard for human life, instead of hardened military targets.

The national security mission of today, however, is complex. It involves too many entities and it is not possible to bring them all under one roof. The network approach would be a better fit for Singapore. This network, though, would need direction and coordination from a central hub that has sufficient influence to motivate constituent agencies. In short, the organizational challenge of national security is to mobilize, coordinate and lead government agencies, the business community and the general public to make Singapore better prepared, more secure and more responsive to an array of threats.

To fight the terrorist threat in the long haul, the Government has adopted a multi-ministry networked approach. Networking integrates the work of otherwise separate bodies, enables inter-agency coordination and allows us to leverage upon the strengths of diverse organizations. No single agency will have all the resources or capabilities needed to handle the range of threats at all levels. The real emphasis should be on cultivating a culture of collaboration. Army/Police patrols at Changi Airport are a practical example of inter-agency coordination and convergence. We have to nurture a propensity to think about how we can achieve more as a team even as we play our functional roles.

Three essential security pillars are policy, operations and capability development. A Permanent Secretary for National Security and Intelligence Coordination has been appointed to head the Secretariat. The Government will strengthen risk-assessment and horizon-scanning capabilities to bring together different agencies in the tasks of monitoring and authoring scenarios, assessing risks and sounding early warnings. We will also work with think-tanks and research institutes to develop a common, in-depth understanding of the terrorism problem, especially its ideological underpinnings.

To deal effectively with the threat of transnational terrorism, Singapore has deployed a robust defence strategy built upon a well-organized network of government agencies, often working in partnership with commercial and private parties. This integrated, layered approach is structured around the Prevention, Protection and Response domains. One critical component in combating transnational terrorism is good intelligence. Also, strong controls at the

borders of the country and enhanced security of Singapore's critical infrastructure.

We have to prioritize our efforts, given our limited resources, and focus on areas of greatest concern. Singapore's status as an international aviation hub is not just a source of national pride, but is also the foundation on which much of the economy rests. It is a vital asset that must be well guarded.

At Changi Airport, access to restricted areas of the airport, aircraft and other key installations is guarded and closely monitored. The Police and SAF mount joint patrols of the airport concourse and other sensitive areas. All checked-in baggage is also screened through an in-line baggage screening system.

Many of our current preventive, protective and response capabilities are based on good use of the latest technology.

Technology specific to the counter-terrorism programme is one domain where, currently, possibly the greatest potential for development rests.

Defending Singapore is the Government's most fundamental commitment to its citizens.

As long as we remain a secular state that represents modernity and progress, we will find ourselves standing against the extremist visions of terrorist groups.

Prime Minister Goh Chok Tong has also emphasized that *'every community must speak up against extremist voices that sow racial and religious discord among Singaporeans.'* Shortly after the September 11 attacks, Singapore established Inter-Racial Confidence Circles (IRCCs) to promote multi-racialism and inter-communal harmony. To date, IRCCs have been formed in all 84 constituencies in Singapore.

Annex 11

Recommendations from the USA 9/11 report, 2004

Extracts from recommendations in the *Final Report of the National Commission on Terrorist Attacks upon the United States, W.W Norton, 2004,* which have potential relevance to the Review by the Rt Hon Sir John Wheeler DL are outlined in the following text.

The terrorist attacks on September 11, 2001, in the United States had a massive impact on American determination to counter terrorism. Since the attacks, the United States has acted to sharpen and bolster its counter-terrorism arrangements. One area where security and counter-terrorism measures have been improved is in the aviation sector.

The final report of the independent, bipartisan commission created by Congressional legislation under the signature of President George W. Bush in late 2002 produced recommendations in 2004 which include:

- As the President determines the guidelines for information sharing among government agencies and by those agencies with the private sector, he should safeguard the privacy of individuals about whom information is shared.
- Hard choices must be made in allocating limited resources. The US government should identify and evaluate the transportation assets that need to be protected, set risk-based priorities for defending them, select the most practical and cost-effective ways of doing so, and then develop a plan, budget and funding to implement the effort. The plan should assign roles and missions to the relevant authorities (federal, state, regional and local) and to private stakeholders.
- Targeting travel is at least as powerful a weapon against terrorists as targeting their money. The United States should combine terrorist travel intelligence, operations, and law enforcement in a strategy to intercept terrorists, find terrorist travel facilitators, and constrain terrorist mobility.
- We should do more to exchange terrorist information with trusted allies, and raise US and global border security standards for travel and border crossing over the medium and long term through extensive international cooperation.
- Secure identification should begin in the United States. The federal government should set standards for the issuance of birth certificates and sources of identification, such as drivers licenses. Fraud in identification documents is no longer just a problem of theft.

- This screening function should be performed by the TSA, and it should utilize the larger set of watchlists maintained by the federal government. Air carriers should be required to supply the information needed to test and implement this new system.
- The TSA and the Congress must give priority attention to improving the ability of screening checkpoints to detect explosives on passengers. Further, the TSA should conduct a human factors study, a method often used in the private sector, to understand problems in screener performance and set attainable objectives for individual screeners and for the checkpoints where screening takes place.
- At this time of increased and consolidated government authority, there should be a board within the executive branch to oversee adherence to the guidelines we recommend and the commitment the government makes to defend our civil liberties.
- Homeland security assistance should be based strictly on an assessment of risks and vulnerabilities. It should supplement state and local resources based on the risks or vulnerabilities that merit additional support. Congress should not use this money as a pork barrel.
- Emergency response agencies nationwide should adopt the Incident Command System (ICS). When multiple agencies or multiple jurisdictions are involved, they should adopt a unified command.
- We endorse the American National Standards Institute's recommended standard for private preparedness. Private sector preparedness is not a luxury; it is a cost of doing business in the post-9/11 world.
- We recommend the establishment of a National Counterterrorism Center (NCTC). Breaking the older mould of national government organization, this NCTC should be a center for joint operational planning and joint intelligence, staffed by personnel from the various agencies. The head of the NCTC should have authority to evaluate the performance of the people assigned to the Center.
- Information procedures should provide incentives for sharing, to restore a better balance between security and shared knowledge.
- The President should lead the government-wide effort to bring the major national security institutions into the information revolution. He should coordinate the resolution of the legal, policy, and technical issues across agencies to create a 'trusted information network'.

- A specialized and integrated national security workforce should be established at the FBI consisting of agents, analysts, linguists, and surveillance specialists who are recruited, trained, rewarded and retained to ensure the development of an institutional culture imbued with a deep expertise in intelligence and national security.

Annex 12

Cost of the Review

The Airport Security and Policing Review (ASPR) has an approved budget estimate of $1.476m. Employee remuneration of $0.783m comprises the largest component of the ASPR operating budget, while Suppliers Expenses are around 47 per cent of the overall budget and include the cost of 24-hour security, property-operating and communications/information technology costs of $0.260m. The salary of the seconded officer from the ACC was not funded by the ASPR; however, by agreement all supplier expenses for this officer are paid from the ASPR budget.

Budget actuals will not be able to be finalised until October after the end of the Review in September.

Table 3:
Details of estimates for the period of the Review
7 June 2005 – 30 September 2005

Branch name	Revenue from Gov't $'000	Revenue from other sources $'000	Employee & Supplier expenses $'000	Depreciation and other expenses $'000	Net Operating Expense $'000
ASPR Review Members	$0	$0	$0.600	$0	$0.600
ASPR Secretariat	$0	$0	$0.860	$0.016	$0.876
Total	**$0**	**$1.476**	**$1.476**	**$0.016**	**$1.476**

Personnel

The ASPR estimated its staffing needs based on an expected staffing profile as shown below. The Review expected to commence 2005–06 at near full budgeted levels, but due to the urgent establishment of the Review not all positions were able to be filled immediately; two additional staff and a secondee joined the Review in July and August. Although not shown under employee expenses, the Review contracted a full-time, 24-hours-a-day, security guard, for the duration of the Review. These expenses have been included in the Supplier component.

The proposed FTE was set at 14 and included the three Review Members and Secretariat staff, with additional assistance provided by an EL1 Contractor to coordinate a benchmarking exercise comparing international airport security and policing arrangements with Australian airports. The Review was fortunate to secure the services of an experienced EL1 officer from the Australian Crime Commission (ACC) on secondment for the period of the Review; his salary and

entitlements were covered by the ACC, but he, along with the EL1 Contractor, has been shown in the following table for the purpose of reporting on resources.

Table 4:
Staffing headcount and FTE

Classification	Headcount & FTE	
	June 2005	September 2005
APS1-3	1	1
Graduates	2	3
APS5-6	2	2
ELI & EL2	2	5
SES	2	2
Review members	3	3
Total	**12**	**16**

Annex 13

Biographies of review members and secretariat staff

The Rt Hon Sir John Wheeler, DL
Sir John Wheeler has had an extensive career in public service, and was Member of Parliament from 1979 to 1997, sitting for the City of Westminster, Paddington (1979–1983) and Westminster North (1983–1997).

From 1993 to 1997, Sir John was Deputy Secretary of State, Northern Ireland Office. In this role, Sir John was responsible as Minister of State for Security and the Criminal Justice System and as Finance Minister for a budget of some 8 billion pounds. In those positions, Sir John became intimately aware of the challenges of terrorism and criminality.

As a member of the Home Affairs Select Committee, Chairman of a Sub-committee (1980–1997), and Chairman of a Select Committee (1987–1992), Sir John produced 67 reports. Examples of these reports include a comprehensive inquiry into racial disadvantage after the riots in 1981; the future of Broadcasting in 1987–1988; and from 1987–1991 several inquiries into criminal justice and police policy issues; also in 1988, he was responsible for the recommendation to establish the National Criminal Intelligence Service in the UK.

Sir John has been Chairman of the British Security Industry Association Inspectorate, set up at the request of the Home Office; Deputy Lieutenant of Greater London; and representative Deputy Lieutenant of the London Borough of Merton from 1997. In 1993 he was appointed a Member of Her Majesty's Most Honourable Privy Council. Sir John has been Chairman of The Service Authorities for the National Criminal Intelligence Service, the National Crime Squad, and the Jockey Club Review Group into conflicts of interest.

In 2002, Sir John undertook a review of arrangements for security, including the threat of organised crime, at airports within the UK for the Secretary of State for Transport and the Home Secretary.

Mr John Abbott CBE, QPM

John Abbott is a career law-enforcement officer who has served in a range of operational, managerial and leadership positions at both tactical and strategic levels during his career in the United Kingdom and internationally.

Mr. Abbott recently retired as Director-General of the UK's National Criminal Intelligence Service (1997–2003). He also served as Chairman of the G8 law enforcement group (1997–2002), as the UK representative to the Europol Management Board (1998–2003), and as Vice President and Executive Committee member of Interpol (1999–2002).

Mr. Abbott has had significant experience in tackling organised crime, in countering terrorism, in developing crime prevention and criminal intelligence capabilities, and in critical-incident management. His earlier position as Police Commander at Kai Tak Airport in Hong Kong and at Gatwick Airport in the UK was particularly relevant to the work of the Review.

Mr. Abbott is currently working with Interpol as a specialist adviser and Chairman of Interpol's programme addressing bio-terrorism, as well as being a senior associate tutor at the UK's national police college (Bramshill) focusing on transnational organised crime, terrorism, and strategic leadership. He is also a coach to the EU Police Chiefs Task Force looking at multi-national police cooperation at the EU level, and a specialist advisor to the House of Lords on terrorism and organised crime.

Mr Neil Fergus

Neil Fergus is the Chief Executive Officer of Intelligence Risks Pty Ltd, an international security company specialising in the provision of security advice; of facilities security designs and operational plans; of counter-terrorism risk advice; and of security services for international major events. Intelligent Risks worked in over 30 countries in 2003 alone, and has contracted their services to international major events including the Athens Olympic Games in 2004.

From 1997 to 2001, Mr. Fergus was Director of Intelligence for the Sydney 2000 Olympic and Paralympic Games, and was a key member of the management team for those Olympics.

Prior to moving into private business, Mr. Fergus had an extensive public sector career in the Australian Intelligence Community for over 20 years, serving in a variety of positions in Australia and overseas.

Mr. Fergus is a frequent commentator on terrorism, and has published a substantial number of articles on security and risk issues. He holds both a Bachelor of Arts and a Bachelor of Law degree.

Secretariat

A secretariat was formed to support this Review, comprising ongoing and non-ongoing officers from the Department of Transport and Regional Services, one officer from the Australian Crime Commission, and a technical consultant.

The Review Secretariat was headed by Kym Bills. Mr. Bills was educated at Adelaide University, Flinders University and Oxford University and has also completed postgraduate degrees at the Australian National University and Charles Sturt University. He holds a number of professional fellowships. Mr. Bills has worked in a range of public service agencies since 1978. He was head of the Commonwealth's Maritime Division from 1994 and a member of the Boards of ANL Ltd and AMSA. Since 1 July 1999, Mr. Bills has been Executive Director of the newly formed multi-modal Australian Transport Safety Bureau (ATSB).

Senior members of the Secretariat were Dr. Andrew Turner and Dr. W.J. O'Malley.

Dr. Turner has been a member of the Australian Public Service Senior Executive Service since 1988. He joined what is now the Department of Transport and Regional Services in 1997, and has been head of the Aviation Security Branch since January 2002. His doctorate is in geography, awarded by the Australian National University in 1980.

Dr. O'Malley holds a Ph.D. in History from Cornell University, where he also studied Government and Economics at the post-graduate level. He has worked at various universities, most recently in 2000 when he was Visiting Professor in International Studies at the Virginia Military Institute. Dr. O'Malley worked at the Office of National Assessments from 1986 until 2004, retiring as Assistant Director-General.

Other members of the Secretariat were: Executive Level Officers Mrs Jane Hanna; Ms Gabrielle Crick; Mr Scott Shearer, who was seconded from the Australian Crime Commission; and Mr Kevin Luke, an ICAO Universal Security Audit Program Certified Team Leader with 22 years of experience in aviation security. Secretarial and administrative staff were: Ms Jill Brooks; Mrs Kay Hart; and Ms Carolyn Shelper. Graduate researchers were Ms Erin Cann; Mr Hamish Hansford; and Mr Daniel O'Malley. Desktop publishing for the Review Report was undertaken by Mr. David Hope of the ATSB.

Annex 14

Acronyms and abbreviations

AAA	Australian Airports Association
ACC	Australian Crime Commission
ACID	Australian Criminal Intelligence Database
ACS	Australian Customs Service
ACT	Australian Capital Territory
ACTU	Australian Council of Trade Unions
ADF	Australian Defence Force
AFP	Australian Federal Police
AFPPS	Australian Federal Police Protective Service
AGAASC	Australian Government Agencies' Airport Security Committee
AGCTC	Australian Government Counter-Terrorism Committee
AGCTPC	Australian Government Counter-Terrorism Policy Committee
AGD	Attorney-General's Department
AIC	Australian Intelligence Community
ALEIN	Australian Law Enforcement Intelligence Network
ANAO	Australian National Audit Office
ANPR	Automatic Number Plate Recognition
APC	Airport Police Commander
APEC	Asia-Pacific Economic Cooperation
APS	Australian Protective Service / Australian Public Service
AQIS	Australian Quarantine and Inspection Service
ASC	Airport Security Committee
ASIC	Aviation Security Identification Card / Australian Securities and Investments Commission
ASIS	Australian Secret Intelligence Service
ASIO	Australian Security Intelligence Organisation

AS/NZS	Australian Standards and New Zealand Standards
ASO	Air Security Officer
ASPR	Airport Security and Policing Review
ASVS	Australian Security Vetting Service
ATSA	Aviation Transport Security Act 2004
ATSB	Australian Transport Safety Bureau
ATSR	Australian Transport Security Regulations 2005
AUSTRAC	Australian Transaction Reports and Analysis Centre
AVSEC	Aviation Security
BAC	Brisbane Airport Corporation
BARA	Board of Airline Representatives of Australia
CATSA	Canadian Air Transport Security Authority
CBR	Chemical, Biological, Radiological
CCTV	Closed-Circuit Television
CEO	Chief Executive Officer
CIP	Critical Infrastructure Protection
COAG	Council of Australian Governments
CSIRO	Commonwealth Scientific and Industrial Research Organisation
CTFR	Counter-Terrorism First Response
CTO	Cargo Terminal Operator
Customs	Australian Customs Service
DFAT	Department of Foreign Affairs and Trade
DIGO	Defence Imagery and Geospatial Organisation
DIMIA	Department of Immigration and Multicultural and Indigenous Affairs
DIO	Defence Intelligence Organisation
DOTARS	Department of Transport and Regional Services
DSD	Defence Signals Directorate
DSTO	Defence Science and Technology Organisation
EACS	Electronic Access Control Systems

EIDS	Electronic Intruder Detection System
EL	Executive Level
ETD	Explosives Trace Detection
Finance	Department of Finance and Administration
FTE	Full Time Equivalent
GA	General Aviation
GDP	Gross Domestic Product
HVP	High Visibility Policing
ICAO	International Civil Aviation Organization
ICS	Incident Command System
Immigration	Department of Immigration and Multicultural and Indigenous Affairs
IMO	International Maritime Organization
IRA	Irish Republican Army
IRCC	Inter-Racial Confidence Circle
IT	Information Technology
ITS	Inspector of Transport Security
JCPAA	Joint Committee on Public Accounts and Audit
JTF	Joint Task Force
LAC	Local Area Command
LEO	Law Enforcement Officer
MAL	Movement Alert List
MANPADS	Man Portable Air Defence System
MATRA	Multi-Agency Threat and Risk Assessment
MSIC	Maritime Security Identification Card
NASS	National Aviation Screening Standard
NCIP	National Critical Infrastructure Protection Program
NCTC	National Counter-Terrorism Committee
NCTH	National Counter-Terrorism Handbook
NCTP	National Counter-Terrorism Plan

NSC	National Security Committee of Cabinet
NSW	New South Wales
NT	Northern Territory
NTAC	National Threat Assessment Centre
ONA	Office of National Assessments
OTS	Office of Transport Security
PIRA	Provisional Irish Republican Army
PM&C	Department of the Prime Minister and Cabinet
PNG	Papua New Guinea
PSCC	Protective Security Coordination Centre
PSLO	Protective Security Liaison Officer (in the AFP)
PSO	Protective Service Officer (from AFPPS)
QANTAS	Queensland and Northern Territory Aerial Services Limited
QLD	Queensland
RAAA	Regional Airlines Association of Australia
RACA	Regulated Air Cargo Agent
RPT	Regular Public Transport
RRDT	Regional Rapid Deployment Team
SA	South Australia
SACL	Sydney Airport Corporation Limited
SAF	Singapore Armed Forces
SCNS	Secretaries' Committee on National Security
TAS	Tasmania
TISN	Trusted Information Sharing Network
TSA	Transportation Security Administration (within the United States Department of Homeland Security)
TSP	Transport Security Program
UN	United Nations
VIC	Visitor Identification Card
WA	Western Australia