Questions on notice from JCPAA hearing on 5 December 2005

QUESTIONS ON NOTICE

Question 1

Departures from ICAO standards
Prohibited items

- When will Australia next review / report on the list of prohibited items?

The International Civil Aviation Organization (ICAO) provides guidance to aviation industry participants on what constitutes prohibited items. This guidance is contained in Appendix 35 of ICAO's Security Manual for Safeguarding Civil Aviation Against Acts of Unlawful Interference (a restricted document).

Prohibited items are defined in the manual as 'those articles that must never be carried in the cabin of an aircraft or taken into the Security Restricted Area of an airport except by authorized persons who require them to undertake essential tasks'. The ICAO manual provides five generic categories of prohibited items. These categories can be used to assist in identifying items, and are

- Firearms, guns and weapons
- Pointed / edged weapons and sharp objects
- Blunt instruments
- Explosive and flammable substances
- Chemical and toxic substances.

The manual then provides examples of items that may be classed in each of these categories. These listings are not all inclusive.

ICAO's prohibited items list is intended to provide guidance only. It is up to individual States to establish their own prohibited items list, based on their own risk assessments. ICAO also provides a further list of items that States may wish to include on their prohibited items listings, including corkscrews, knitting needles, metal cutlery and blades of less than 6 cm.

The following table provides some examples for comparison of prohibited items policies in a number of countries.

ICAO listing	Australia	New Zealand	USA	UK	Canada
Scissors	Manicure scissors and scissors with blades more than 6 cm long may be carried in checked baggage. Blunt or round-ended scissors with blades less than 6 cm long may be carried in cabin baggage	Blades less than 6 cm permitted in cabin baggage	Scissors with blunt tips (blades no longer than 4 inches) permitted in cabin baggage	Blades less than 6 cm permitted in cabin baggage	Scissors with pointed tips may only be carried in checked baggage
All firearms – must not be loaded	May be carried in checked baggage	May be carried in checked baggage	May be carried in checked baggage	May be carried in checked baggage	May only be carried in checked baggage if approved by carrier
Sporting equipment	May be carried in checked baggage	May be carried in checked baggage	May be carried in checked baggage	May be carried in checked baggage	May be carried in checked baggage
Martial arts equipment	May be carried in checked baggage	May be carried in checked baggage	May be carried in checked baggage	May be carried in checked baggage	May not be carried
Grenades of all types	May be carried in checked baggage	May be carried in checked baggage	May not be carried	May be carried in checked baggage	May not be carried
Fire extinguishers		May be carried in checked baggage		May be carried in checked baggage	May not be carried
Cutlery	Metal cutlery may be carried in checked baggage		Plastic or round bladed non-serrated butter knives may be carried in checked baggage	On-board metal cutlery must conform to certain design criteria	Kitchen forks permitted
Knitting and crochet needles	May be carried in checked baggage		May be carried in checked baggage		May be carried in cabin baggage
Replica, imitation or toy firearms	May be carried in checked baggage	May be carried in checked baggage	May be carried in cabin baggage if not 'realistic replicas'	May be carried in checked baggage	May be carried in checked baggage

The Office of Transport Security provides constant advice to the Australian Government, and operates an intelligence driven, risk based security system.

The Office of Transport Security is currently undertaking a review of the recently introduced *Aviation Transport Security Act 2004* and the *Aviation Transport Security Regulations 2005*. The prohibited items list will be considered in the context of this review. This issue is also being considered by a working group established under the framework of the Aviation Security Advisory Forum.

The Department of Transport and Regional Services will provide a report to government in June 2006 with suggested policy changes identified in the legislative review process. This report will include the issue of the prohibited items list.

Question 2

Delays in getting ASIC approvals

- What is DOTARS doing to improve turnaround times?

One of the challenges faced by DOTARS and by ASIC applicants is the length of time taken to complete background checks. These checks are done by the Australian Federal Police (criminal history check) and ASIO (politically motivated violence check) and, if necessary, a Department of Immigration and Multicultural Affairs unlawful non-citizen check. These checks are usually able to be turned around in two to three weeks.

There are currently a number of factors present with regard to the completion of ASIC background checks that are having a detrimental effect on the turnaround times for these checks. One of these factors is the concurrent processing of applications for Maritime Security Identification Cards, the number of which currently stands at 130,000, as well as the 120,000 ASIC applications in the system at present. Another factor is the need to do background checks on everyone working at the Commonwealth Games.

The Wheeler report addressed the concept of a centralised vetting agency for the processing of ASIC applications. Such an agency would provide greater efficiencies that would likely result in faster processing of ASICs.

DOTARS works closely with ASIO and the AFP to work to improve turnaround times, including through examining electronic data lodgement.

Question 3

Issuing of demerit points for failure to return an ASIC

- Have any demerits of this nature ever been issued?

No. While the *Aviation Transport Security Act 2004* provides for a demerit system, Regulations have not been made to give effect to such a system.

Question 4

Incidents of criminality and audits at SACL

- Provide the Committee with information on rates of incidents at SACL, as well as trend data from DOTARS audits

Incidents at SACL

The Office of Transport Security's Operations Centre recorded details of the 1768 aviation security related incidents that occurred at Australian airports in 2005.

There were approximately 60 million aircraft passenger movements in 2004-05. Statistics provide by the Bureau of Transport and Regional Economics show that 25 per cent of domestic passenger movements involve a connection with Sydney. Passengers travelling internationally to or from Sydney account for 47 per cent of total international passenger movements.

In 2005, 301 of the security incidents reported to the Office of Transport Security's Operations Centre occurred at Sydney Airport. This is 17 per cent of the total number of incidents reported. This number is proportionally less than the airport's share of passenger numbers.

The Office of Transport Security uses a three tier system for categorising incidents. Of the incidents recorded at Sydney Airport, over 96 per cent were classified as Level 1 security incidents. Incidents classified at this level are those that have a very low probability of endangering the security of people and assets or of reducing public confidence in aviation security. Such minor issues will generally not disrupt aviation operations.

The Office of Transport Security works with airports such as Sydney Airport to reduce the number of security incidents where possible. However, even the best security arrangements will not stop certain members of the public from making 'jokes' and trying to open locked doors.

The Office of Transport Security does not capture information relating to incidents of a criminal nature at airports, and suggests that the Committee seek such information from agencies such as the Australian Federal Police or the Australian Crime Commission.

Trend data from audits at SACL

The Office of Transport Security conducts an annual audit of Sydney's international airport. The audits for 2004 and 2005 were examined to identify if trends were observed in relation to the security performance of the airport.

A number of issues were identified in each audit and brought to the attention of Sydney Airport Corporation Ltd for action. SACL advised, in a timely manner, what immediate action had been taken against each item, as well as outlining longer term strategies where necessary / appropriate. Only one common issue was identified across both years, involving access to tools of trade in the concessionaires' areas of the passenger terminals.

Other areas for improvement identified in the audits included insufficient signage to warn about leaving baggage unattended, documentation left by airline staff in unattended gate lounges, training of operations staff and contracted security guards, and minor fenceline / perimeter issues.

Question 5

Audits – structure of Airport Security Committees

The Airport Security Committees in place at Australia's major airports meet regularly and are effective.

The requirements for an Airport Security Committee are specified in each airport's Transport Security Program (TSP), as required by Regulation 2.11(3) of the *Aviation Transport Security Regulations 2005*. This is assessed during airport audits.

Recommendation VII of the Wheeler review into airport security and policing arrangements provides some guidance to airports as to the structure and role of the committees, which Wheeler recommended be renamed Airport Security Consultative Groups at the CTFR airports. It is possible for an airport to have a separate high level group, the details of which would be included in the airport's Transport Security Program.

As well as these committees, the Department has established Australian Government Agencies' Airport Security Committees (AGAASCs) in major Australian airports. These committees contribute a mechanism for policy integration and discussion at the Australian Government level, as well as the sharing of information and coordination of information dissemination.

The role of the AGAASCs is changing with the appointment of a senior Australian Federal Police officer as a security controller at each of Australia's major airports. This officer's role will be to coordinate the operational activities of Commonwealth Government agencies to ensure that our resources are focused on the major priorities with respect to criminal activity at airports. The AGAASCs have implemented informal agreements with Airport Security Committees.

AGAASCs meet on a regular basis, and the minutes of these meetings are an agenda item for the Australian Government Transport Security Policy Committee meetings. AGAASC meetings are typically attended by representatives of DOTARS, the Australian Customs Service, the Department of Immigration and Multicultural Affairs, the Australian Quarantine Inspection Service and the Australian Federal Police Protective Service.

Question 6

Information available through the passport/visa management system

- Automatic transfer of information from country of origin to country of arrival

Overview

The Advance Passenger Processing (APP) system allows airlines to verify, at the check-in point, that all types of travellers, including passengers and crew members, have authority to enter Australia. The system sends the advance passenger information to the destination country prior to the person boarding their flight or vessel using global communication networks. The system was introduced in Australia to manage the growth in numbers of visitors and to enhance border control.

The *Australian Migration Act 1958* was amended in 2002 to allow Australia the capability to require advance passenger information from aircraft and ships entering the country. The legislation puts an obligation on specific types of aircraft and ships to provide information on all passengers and crew members entering Australia within a specific time frame. Penalties are in place for failure to comply.

The provision of advance reports of passengers and crew to the Department of Immigration and Multicultural Affairs has been mandatory for all airlines since 5 January 2003 and cruise ships since 1 January 2004.

Capabilities of the APP system

The system advises the government of the destination country/ies of a passenger's intention to travel internationally and, in response, receives a boarding directive from those governments confirming whether or not the passenger can board (ie Australia or New Zealand). The checking takes place in real time whilst the passenger is going through the airport check-in process. The APP system may direct the airline to: board the passenger or crew member, not allow the passenger or crew member to board, or be referred to the relevant 24 x 7 operational centre.

The APP is not limited to scheduled flights – it can also be used for unscheduled and charter flights.

Using the information collected by immigration authorities, governments perform detailed checking and profiling prior to the passenger or crew member arriving, and are able to plan and prepare for interventions in cases of interest.

Besides passports, the APP system can handle all types of travel documents, including Certificate of Identity, refugee travel documents, United Nations documents, Seaman's' books and other forms of military identification.

Most airlines utilising the APP system have integrated it into their Departure Control System, (based on system specification outlined by the System Provider), to ensure that passengers are not boarded without successful APP checks being undertaken.

However, it is up to individual airlines to determine how the APP functionality is integrated into their systems.

Capturing of passenger information

Most airlines capture passenger information at the time of ticket purchase. This information is stored in the Computer Reservation System. Upon check-in the data taken from the passenger's passport is forwarded via the APP system for checking against DIMA's data and alert systems, thus allowing for the issuing of boarding directives to check-in staff. This process results in the creation of an 'expected movement record' (EMR), which is sent to DIMA. These EMRs are swept by DIMA every two minutes and are then forwarded to DIMA's agent, the Australian Customs Service (Customs), to be used for processing the passenger upon arrival at the Australian border.

The APP system allows for the capturing of the following passenger details:

- Travel document number
- Travel document ICAO country code
- Family name
- Given name/s
- Date of birth
- Gender
- Trans-border (international) flight
- Check-in port
- Expected port
- Check-in date
- Trans-border port *

* The trans-border port is defined as the first port at which a passenger arrives when travelling to that country or the last port from which a passenger departs when travelling from that country. For example, in the case of a passenger flying into Sydney's international terminal and then catching a domestic flight to Canberra, the trans-border port is Sydney.

Passenger names are cross-checked against an alert list. A notification message is automatically generated if the system detects a match. This notification message is printed to a processing centre for advice.

The information Customs receives from DIMA is collected in the Passenger Analysis, Clearance and Evaluation System and stored as 'expected arrivals'. When the passenger has physically arrived in the destination country and has cleared the Customs process, the 'expected arrival' record is re-categorised as an 'actual arrival'.

Compliance

There are currently fifty commercial airlines flying scheduled services into Australia that are utilising the APP system with compliance at around 99 per cent. The

Australian Government is working closely with these airlines to obtain 100 per cent compliance with the APP system.

Question 7

Storage of data from images captured in airports

- Passengers with their luggage, for comparison purposes later if required
- Images of baggage taken during screening process for comparison purposes later if required

The x-ray technology currently in use in Australian airports allows the airline to identify baggage that may contain a firearm or explosive item. Current systems have not been designed to effectively identify any other items such as drugs or contraband.

Most currently deployed technology does not have the capability to record and retain images for a prolonged period, or to export images to other IT systems. It is not possible to simply connect an image storage centre to a baggage x-ray screening device.

Qantas has acquired new x-ray machines with 'multi-view tomography' (MVT) for its domestic terminals at Sydney, Melbourne, Perth and Brisbane airports. These machines have the capability to record 100,000 images, subject to certain limitations. These machines are to be progressively deployed by Qantas to the other seven Counter-Terrorism First Response airports. Other terminal operations may use different equipment with different retention capabilities.

The MVT technology is capable of storing only a certain number of images and once the system has reached capacity, the oldest images will be replaced under the 'first in, first out' principle. It is not possible to state how long it will take the system to replace the oldest images, as this will be determined by the throughput of bags. Images may be able to be stored for as long as 10 days, but during peak periods such as school holidays and Christmas this may be reduced to as few as five days. Older technology may have more limited image retention capability.

It is important to note that the MVT system can only retain images of baggage that pass through the x-raying facilities. Oversized luggage is screened differently, utilising a combination of explosive trace detection and physical search which do not result in the taking or storage of x-ray images.

The utilisation of such equipment is not inexpensive. Currently, in order to download an image from the system for permanent record, a technician must be engaged to attend the site to facilitate the retrieval. This incurs a call-out fee of several hundred dollars. Increasing the storage capacity of the MVT machines would involve the installation of a dedicated server to assist in the downloading of images, allowing a longer overall retention period for the images. Such a server is estimated to cost tens of thousands of dollars per machine. Integration between the MVT and baggage x-ray machines would incur substantial costs in the areas of process re-engineering, software re-programming and data collection, and storage and retrieval protocols. It is not possible to estimate such costs at this time.

There would be business process changes associated with any proposal to enhance the image retention capability of currently utilised baggage x-ray machines, including the time and financial costs of operator training and the disruption to business in the event that a machine needs to be isolated to facilitate the downloading or transfer of images.

Any increase in the technical complexity of the baggage x-ray process is likely to also increase screening times, which may have a significant business impact on both terminal operators and carriers through delays to operations and screening point bottlenecks. This in turn could result in passenger frustrations.

With regards to the domestic context, it is important to recognise that not all Australian ports use the same technologies and equipment – it would not be possible to implement a one size fits all solution. Each port where airlines screen baggage would require its own specific technology. Unless a single central storage facility throughout the domestic network was established, the system would operate at each port in isolation and to differing standards.

The storage of baggage images would not create any significant security outcome or benefit considerate of the cost and the ongoing technical developments and advancements.

ADDITIONAL QUESTIONS FROM THE COMMITTEE

Question 1

Could you identify the procedure by which security classified airports are assigned their status and the processes used to determine what security measures will be required at each security classified airport?

<u>Procedure by which security classified airports are assigned their status</u>

In the development of the *Aviation Transport Security Act* 2004 and the *Aviation Transport Security Regulations* 2005, the Australian Government assigned airports with a security controlled status following consideration of current threat assessments, including those prepared by the Australian Security Intelligence Organisation. Consultation was also undertaken with state and territory governments.

Generally, an airport will be given security controlled status if it receives regular public transport services or is a major general aviation airport close to a significantly sized metropolitan area. All security controlled airports are required to be gazetted in the Public Service Gazette.

Airports that commence receiving regular public transport services will be gazetted as security controlled.

<u>Counter-Terrorism First Response airports</u>

Counter-Terrorism First Response (CTFR) airports are not specifically defined in the *Aviation Transport Security Act 2004* and the *Aviation Transport Security Regulations 2005*, but are designated under Regulation 3.27 for the purposes of CTFR provisions. These same 11 airports are listed in Regulation 2.23 as ‘major airports’.

These 11 airports carry a greater risk from terrorist activities and consequently are required to implement greater security measures, including hosting Australian Federal Police (AFP) CTFR capabilities. Major airports are attractive targets for terrorists for a number of reasons, including the concentration of large number of people at predictable times, the provision of access to large commercial jets, their national and economic symbolism, operational complexity and the greater potential consequences of such an attack.

A full listing of security controlled airports is at **Attachment A**.

<u>Processes used to determine what security measures will be required at each security classified airport</u>

In addition to the requirements generally of security controlled airports under the *Aviation Transport Security Act 2004* and the *Aviation Transport Security Regulations 2005*, operators of security controlled airports are required to develop a Transport Security Program. This program includes a security risk assessment specific to that airport, as well as the security measures the operator will implement to address those risks identified in the risk assessment.

CTFR airports, due to the nature of their operations, employ additional measures such as checked baggage screening procedures and improved access controls.

Question 2
Can you provide a timeline relating the dates on which the numbers of security regulated airports have increased and the criteria used to increase the number of security regulated airports on each occasion?

Under the *Air Navigation Act 1920*, 40 airports were classified as security controlled airports. These transitioning airports are shown on the airport list at Attachment A. With the introduction of the *Aviation Transport Security Act 2004* and the *Aviation Transport Security Regulations 2005* on 10 March 2005, all airports that received regular public transport services became security controlled and were gazetted accordingly.

Since 10 March 2005, three further airports have been classified as security controlled airports – Illawarra Regional, Argyle and Kempsey.

The criteria used to classify airports as security controlled was outlined in the response to Question 1 (above).

Question 3

Can you explain the basis on which airports with Regular Public Transport services automatically become security classified?

The security controlled classification of airports receiving regular public transport services is consistent with the risks identified in the aviation industry’s threat assessment, referred to in our response to Question 1.

Question 4

Do the criteria you employ to security classify airports provide any flexibility to distinguish between airports with a low volume of passengers and those with a higher volume?

No. However, as part of their Transport Security Program, airport operators are required to identify local risk factors and the measures that will be implemented to respond to these.

Question 5

Are factors such as the remoteness of the flight’s origin and destination from potential terrorist targets taken into account in determining which airports will be security classified and what measures will be required?

No, but the risk factors referred to in Question 4 apply.

With regards to international services, the Office of Transport Security works with a number of international partners, including the governments of countries in South East Asia and the Pacific that are last ports of call for commercial services to Australia, to build capacity and to meet international obligations.

Question 6

On 24 November a representative of Linfox, which operates Avalon and Essendon airports, stated that “Our Avalon airport facility did not meet the criteria for [Commonwealth funding of security upgrades] but our Essendon airport did”. Could you explain why a general aviation airport such as Essendon is deemed to require security upgrades whereas a facility that has domestic Regular Public Transport services, including jets, and is capable of taking international services did not qualify?

Regional airports such as Avalon Airport were regulated under the previous legislation, the *Air Navigation Act 1920*, prior to the introduction of the *Aviation Transport Security Act 2004* and therefore already had the appropriate basic security infrastructure to comply with new security requirements.

The assistance available through the Regional Airport Funding Program is currently available only to those eligible airports that are new to the regime to implement basic security measures such as fencing, lighting and alarm systems.