COMMONWEALTH OF AUSTRALIA

Official Committee Hansard

JOINT COMMITTEE OF PUBLIC ACCOUNTS AND AUDIT

Reference: Review of aviation security in Australia

FRIDAY, 5 SEPTEMBER 2003

CANBERRA

BY AUTHORITY OF THE PARLIAMENT

INTERNET

The Proof and Official Hansard transcripts of Senate committee hearings, some House of Representatives committee hearings and some joint committee hearings are available on the Internet. Some House of Representatives committees and some joint committees make available only Official Hansard transcripts.

The Internet address is: **http://www.aph.gov.au/hansard**

To search the parliamentary database, go to: **http://search.aph.gov.au**

JOINT COMMITTEE OF PUBLIC ACCOUNTS AND AUDIT

Friday, 5 September 2003

Members: Mr Charles *(Chairman)*, Senators Conroy, Humphries, Lundy, Murray, Scullion and Watson and Mr Ciobo, Mr Cobb, Mr Georgiou, Ms Grierson, Mr Griffin, Ms Catherine King, Mr Peter King, Ms Plibersek and Mr Somlyay

Senators and members in attendance: Mr Charles, Mr Cobb and Ms Grierson

Terms of reference for the inquiry:

To inquire into and report on:

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

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

(c) compliance with Commonwealth security requirements by airlines;

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

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

(f) privacy implications of greater security measures; and

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

WITNESSES

Committee met at 9.38 a.m.

FRENCH, Dr Greg Alan, Assistant Secretary, Legal Branch, Department of Foreign Affairs and Trade

HUTCHESSON, Mr Bryce David, Assistant Secretary, Antiterrorism and Intelligence Policy Branch, Department of Foreign Affairs and Trade

NASH, Mr Robert John, Assistant Secretary, Passports Branch, Department of Foreign Affairs and Trade

POULOS, Ms Maria, Executive Officer, Department of Foreign Affairs and Trade

SMITH, Mr Paul Manaccan, Director, Protection, Privileges and Immunities Section, Department of Foreign Affairs and Trade

WARD, Ms Elizabeth Harcourt, Director, Business Facilitation and Secure Trade Section, APEC Branch, Department of Foreign Affairs and Trade

WHITE, Mr Damian Craig, Executive Officer, International Law and Transnational Crime Section, Legal Branch, Department of Foreign Affairs and Trade

CHAIRMAN—I declare open the public hearing. I advise witnesses that the hearings today are legal proceedings of the parliament and warrant the same respect as proceedings of the House itself. The giving of false or misleading evidence is a serious matter and may be regarded as a contempt of parliament. Evidence given today will be recorded by Hansard and will attract parliamentary privilege. I refer any members of the press who are present to a committee statement about the broadcasting of proceedings. In particular, I draw the media's attention to the need to report fairly and accurately the proceedings of the committee. Copies of the committee statement are available from secretariat staff. I welcome the witnesses from DFAT. Do you have any comments to make on the capacity in which you appear?

Ms Poulos—I am from the arms control branch.

Mr Hutchesson—I am the head of the DFAT delegation.

Mr Smith—I am in the protocol branch.

CHAIRMAN—Thank you very much for coming and thank you very much for your submission. Do you have a very brief opening statement, or may we proceed to our important questions?

Mr Hutchesson—We do have an opening statement.

CHAIRMAN—Will it be very brief?

Mr Hutchesson—It runs to a page and a half. I can table it if you would prefer.

CHAIRMAN—Go as quickly as you can.

Mr Hutchesson—As the committee would be aware, this department is not a central player on domestic or associated aviation security matters. But the committee's terms of inquiry, encompassing the impact of overseas security requirements on Australian aviation security, suggest it would be useful for us to outline the ways in which the department complements the work of other Australian government agencies on international aviation policy matters that bear on our national security. You have seen our submission, which touches on three key areas of our activity: providing legal advice on international agreements relating to aviation security; coordinating capacity building efforts through APEC to improve regional aviation security standards; and protecting the privileges and immunities of diplomatic and consular officers accredited to Australia, without compromising aviation security arrangements.

Along with the Attorney-General's Department, we advise on Australia's obligations under the four multilateral counter-terrorism instruments relating to aviation security that are mentioned in the submission. We support negotiations on bilateral air service agreements, which generally include aviation security provisions, and we continue to work with other key agencies, particularly in the Attorney-General's portfolio, to extend Australia's domestic air security officer program to other countries and international flights.

The department is responsible for coordinating Australia's involvement in APEC and supports DOTARS's lead in progressing aspects of APEC's secure trade agenda, including the areas of baggage screening, air cargo security, flight deck door standards and broader aviation security audits under ICAO auspices. In addition, we assist DIMIA in elaborating through APEC important initiatives relating to advance passenger information and regional immigration alert systems, although we do recognise that this DIMIA led work relates more to border security than aviation security, strictly defined.

We consult with DOTARS and others on the need to implement security measures, having due regard to our obligations under the Vienna Conventions on Diplomatic and Consular Relations. We do not believe that these conventions require us to compromise on our security procedures but rather that our aviation security procedures should be implemented in a way that recognises the need to respect the inviolability, where it exists, of foreign based diplomats and consular officials here. Our submission did not mention our close involvement in ongoing international efforts to control the production and proliferation of MANPADs, but, given the potential use of these weapons by terrorists and the risk they pose to civil aviation, it is important that the committee be aware that this is an aspect of aviation security that is of interest and relevance to us. Several of the department's travel advisories, particularly but not only for east Africa, refer to the possibility of terrorist attack against airports and civil aviation more generally. The current advisory for Kenya, for instance, refers quite specifically to threats to civil aviation from shoulder-fired missiles.

Finally, although it is a matter again that relates perhaps more to border security than aviation security specifically defined, the committee might be interested in the department's work to incorporate biometrics into Australian passports. There has been encouraging progress on this front. The adoption by ICAO of facial recognition as the international standard for biometric identifiers in passports has left us well placed to move to implementation, subject to successful testing. Parallel to this, a new Australian passport with new and enhanced security features is due

for release this December. I will conclude at that point. We are happy to discuss any of these matters and take any questions from the committee.

CHAIRMAN—Thank you very much, Mr Hutchesson. Before I continue, I simply want to advise those who happen to be watching this on monitors and the observers in the room that there was an incident reported on radio this morning—I think it was *AM*—that Customs computers were stolen from Sydney airport last week, I believe—at least I think that is what I heard on the radio. We interviewed Customs at this hearing yesterday and they did not mention it. My colleague and I have, through our secretariat, requested Customs to reappear in front of the committee to answer very serious questions, so at some point we will be interrupting the advertised schedule of these proceedings today.

We understand that you think you are not a major player. We do not necessarily agree with you; we think you have an important role to play. I have never read a spy thriller that offered some risks in aviation in some country or countries that did not involve foreign affairs departments in some countries or in many countries. Clearly you have a role to play, and I am sure you do play a role with ASIO and other intelligence gathering organisations as well. You may not want to talk about that on the record, but we know that you do have an involvement in this area. You said that our bilateral air service agreements generally include an aviation security clause. To what extent does DFAT monitor those agreements in real time?

Dr French—Generally speaking the role of this department is in advising the lead agency, which is DOTARS, in negotiating such agreements. Once those agreements are completed, generally our role, certainly in the legal area of DFAT, is to advise on interpretation of those agreements. The day-to-day working of and implementation of such agreements is generally with the operational agency.

CHAIRMAN—But you have embassies in every country that we fly into or out of. Does DFAT have a view about where we stack up in the world of aviation security? Where do some of our major regional trading partners stand in some kind of pecking order or hierarchy?

Mr Hutchesson—I will respond to that, Mr Chairman. While I would say that the answer to that would most properly come from DOTARS, we believe that Australia's aviation security arrangements are very robust and compare very favourably internationally. It is also fair to say that in our region there are some countries, some airports and some systems where the standards are perhaps not as high or as rigorously applied as we would like. Part of the work that DOTARS and other agencies do, including to some extent this department, is to work with other countries within existing resources to try to improve, where necessary, the security arrangements in those countries.

CHAIRMAN—Mr Hutchesson, I can understand that you say that DOTARS has the lead, but that does not really absolve you. If you have got embassies in a country and you have staff there, you have a very great responsibility to those staff and those personnel that fly in and out. In addition to that, if my colleague, Mr Cobb, and I fly into Bangkok or Hong Kong or Beijing, you would want to know that we have a reasonable chance of getting there alive and out alive.

Mr Hutchesson—That is absolutely true.

CHAIRMAN—If you think you do not have a responsibility in that regard, well I know that you are wrong.

Mr Hutchesson—What we have a responsibility for doing is certainly drawing to the attention of the Australian travelling public—whether they be politicians, officials, business people, holidaymakers or others—the fact that in certain countries risks do exist from terrorist attack, whether it be to airports or civil aviation or in hotels, bars and the like. Our travel advisory system does point out those risks very rigorously. Along with other relevant Australian government agencies, we certainly do report back from time to time on security arrangements and security situations in the countries where our embassies and high commissions are located. The information that is provided through those reports is digested by those agencies that are most directly involved in aviation security and, in some instances, that will lead to capacity-building work and dialogue on ways to enhance security in those countries.

CHAIRMAN—When you gave your opening statement, you talked about biometric identifiers. What are they?

Mr Hutchesson—Mr Nash will respond to that.

Mr Nash—Biometric identifiers are a means by which people can be recognised. Put simply, it is a system of measuring parts of the human body, capturing those measurements and putting them, in our case, into the passport by the use of chip technology. The system that has been chosen by us—and has now been adopted by the rest of the world—is facial recognition technology. That essentially is the capturing of a whole lot of measurements of the human face and having those transformed to an algorithm. It would be done in such a way that the algorithm, which would be contained on a chip within the passport, would be compared with the photograph, subsequently converted to an algorithm, of the person who appears before a border control point.

CHAIRMAN—How many different measurements will there be?

Mr Nash—There will be several hundred different measurements.

CHAIRMAN—Good grief! So I am not able to fool it by stuffing cotton into my cheeks?

Mr Nash—Unfortunately no—or fortunately.

CHAIRMAN—I do not know why that would be unfortunate. How far are we progressed?

Mr Nash—We are certainly well progressed as far as the testing that we have been doing is concerned. We consider ourselves to be world leaders and have been acknowledged as world leaders in the development of this technology. Other countries are coming along; other countries are dealing with us on a daily basis with regard to the development of this technology. It was adopted as an international standard by the International Civil Aviation Organisation in May. Since then a number of countries have already indicated that they will be proceeding along the same track that we are currently proceeding along—that is, they hope within the next year or so to be in a position to put a microchip into their passports, as we would hope to be able to do.

CHAIRMAN—You have some involvement with the Air Security Officer Program. Is that right?

Mr White—Yes, that is right. I can speak on this issue.

CHAIRMAN—Would you firstly tell us what your involvement is?

Mr White—DFAT has been working with a range of other departments, including the AFP and DOTARS, to progress the arrangements for an international Air Security Officer Program. I understand that a domestic Air Security Officer Program run by the AFP has been going for some time. DFAT has had a twin role in this process. My branch—the Legal Branch—has been giving legal advice to other departments about the negotiations between Australia and Singapore and Australia and the United States. We have also given advice from the bilateral perspective on the relationships with these countries and have advised about progressing the negotiations.

CHAIRMAN—Are you able to tell us where we stand?

Mr White—Yes. We can say that the negotiations with Singapore and the United States are fairly well advanced. There is an agreement between these countries to progress on a non-treaty basis, so the arrangements will be done through an exchange of diplomatic notes. We expect that these negotiations will be finalised fairly soon.

CHAIRMAN—Could you tell us if air marshals in the United States carry weapons?

Mr White—Yes, they do. My understanding is that they do.

CHAIRMAN—Are the weapons firearms?

Mr White—I do not know the specifics of this. You will have put those questions to the AFP.

CHAIRMAN—We should do that. Do our air security officers carry firearms?

Mr White—They will be armed; but again, on operational issues I would recommend that you put the questions to the AFP. We do not give advice on operational issues.

CHAIRMAN—Through your international experience—and you have more than any other department in this place, I think—are you familiar with Tasers?

Mr White—No, Mr Chairman.

CHAIRMAN—Do you know what a Taser is?

Mr Hutchesson—I am taking a guess: are they stun guns?

CHAIRMAN—Yes. It does not touch the individual, but the electronic shock wave does, and it does lay you very flat, very fast. I know—I was an experiment.

Mr JOHN COBB—I must admit that I am a little disturbed. It sounds like a very casual relationship that you describe between yourselves and DOTARS. I cannot believe it is. Do you have regular meetings with them on anything to do with security at airports?

Mr Hutchesson—Not on domestic security arrangements at Australian airports, no, Mr Cobb.

Mr JOHN COBB—Do you not ever look at the possibility that there might be a greater threat, at some stage, to Darwin, Townsville and areas of Sydney, simply because of location or whatever? You do not ever discuss those things with them?

Mr Hutchesson—We are the Department of Foreign Affairs and Trade, which means that our remit is essentially external. We recognise that external circumstance impacts on Australia—that is why the department exists. But when it comes to dealing with the specifics of security at Australian airports, apart from the border security dimensions mentioned by Mr Nash, that is not really a matter for this department.

Mr JOHN COBB—I think you should be very concerned about it. Whether through ASIO or yourselves directly, I would have thought you would have a great input into what DOTARS have to be concerned about and where, and I must admit that I am somewhat disturbed that it does not sound like you are more onto it. What about in the area of cargo, which comes back to trade? That is an area that people are worrying more about. Do you converse with DOTARS about any particular areas? Do you have any more to do with them on trade, perhaps, as far as cargo goes, and maybe passenger aircraft?

Mr Hutchesson—I will ask my colleague Ms Ward to speak to that shortly, Mr Cobb, but certainly in the context of APEC there are a number of initiatives running there. DFAT is the lead agency for coordinating the Australian government involvement in APEC, and there are a number of issues, including cargo security, under APEC auspices. We assist DOTARS in taking those matters forward in the APEC context. Elizabeth, would you like to elaborate on that?

Ms Ward—Over the last couple of years, the department of foreign affairs, which coordinates Australia's activities in APEC—Asia-Pacific Economic Cooperation—has been playing a much more intensive and active role on counter-terrorism related issues. Last year at the leaders summit in Mexico a range of commitments were agreed by leaders to implement counter-terrorism related issues to secure trade through the Asia-Pacific region. These included some issues relating to aviation security, some relating to customs security, some relating to border security—in fact, most of the issues we have been discussing today. On customs related issues and cargo, there was an agreement that all of the Asia-Pacific member economies should adopt the guidelines developed by ICAO and the International Air Transport Association. Also, there was an agreement that there should be some supply chain security guidelines developed and that there should be a range of cargo security issues developed, which would include baggage screening procedures in ports and airports.

Mr JOHN COBB—You have gone on to where I was going. You have touched on it, but with regard to APEC and aviation security, in particular, are there other key issues in security that you are looking at at the moment within our region, with our neighbours?

Ms Ward—The focus this year has been on implementing those commitments that were made last year, which are quite specific at this stage. The focus is really on those individual items that I have mentioned. We have spent time with the various groupings that meet under APEC's auspices to develop ranges of standards so that the entire Asia-Pacific membership is able to carry forward those items knowing that there are standards which apply through the Asia-Pacific region.

Mr JOHN COBB—This committee is very familiar with baggage screening, because we have done quarantine before. Generally, in our region—the APEC region—where are our neighbours up to on promoting 100 per cent baggage screening?

Ms Ward—The commitments we made were for baggage screening as soon as possible and, in any case, by 2005. There are a range of stages of implementation. Every country has provided information on their implementation to date, and where there are gaps in implementation APEC has been developing capacity-building projects to assist member economies to get up to speed.

Mr JOHN COBB—How would we compare to most of APEC in terms of 100 per cent screening? Where would they be in relation to us?

Ms Ward—That very specific question is perhaps better directed to DOTARS. From what DOTARS have told me, I can tell you that Australia's implementation of this particular item—

Mr JOHN COBB—I am aware of where we are up to. I am more interested, in this case, in where our neighbours are up to.

Ms Ward—I think that question needs to be put to the department of transport.

Mr JOHN COBB—You will probably give me the same answer again, but is there more that we can do to encourage or bring up the standard of baggage screening around the region?

Ms Ward—As I said in my previous answer, there are people who are assessing where the gaps are and developing capacity-building projects to assist those economies. That is APEC's core mandate and where we have a comparative advantage in moving forward on these sorts of issues.

Mr JOHN COBB—Mr Hutchesson, are you aware of who the air security officers, the ASOs, are?

Mr Hutchesson—I am.

Mr JOHN COBB—They were introduced subsequent to September 11. Once again, how are we going with extending that program as far as our neighbours are concerned? We were going to discuss with them whether or not they were going to pick up the same program.

Mr Hutchesson—I think Mr White has already touched on that, but he may like to rehearse that again.

Mr White—I can expand on that. Basically, the negotiations in the first instance have been with Singapore, as a regional hub for aircraft coming out of and into Australia, and with the United States, as one of our biggest trading partners.

Ms GRIERSON—You say you have strengthened your work in some areas. One area which I would particularly like to know about is extradition and mutual assistance in criminal investigations. We would see you as having a diplomatic role, I suppose, in negotiations should we have threats or crime in terms of aviation security and terrorism. How difficult is that and how sensitive is it at the moment? What progress has been made? Has it had to change in any way or are you just relying on how things have been for some time?

Dr French—I will mention that the lead role in terms of extradition and mutual assistance lies with the Attorney-General's Department. They have an area there which deals on a daily basis with a whole range of extradition and mutual assistance issues. With regard to those particular issues in the context of aviation security, there is provision in the international agreements to which we are a party providing inter alia for extradition of persons engaged in such activities that are sanctioned by these agreements. They have been implemented in our domestic legislation. So we have fulfilled the requirements of international law through our domestic legislation to ensure that that may be done. That is about the extent of my knowledge of it. I am not aware of specific additional measures with regard to extradition but certainly the measures are in place. As individual instances arise then the relevant parts of the government—led by Attorney-General's, as I said—swing into action.

Ms GRIERSON—You would also take a role in supporting major events and in the planning for major events, such as Commonwealth and Olympic Games. How much involvement would you have in that in terms of Australians travelling intensively at those times and therefore being at heightened risk because of international focus on such events? What role do you play strategically now in preparing for those sorts of activities?

Mr Hutchesson—I might take that question. The department's principal focus in matters of that sort is on the consular front. We work very closely with relevant Australian intelligence agencies, particularly ASIO, in gathering together all the relevant material we can, including material from our posts. That helps us to put together our very extensive program of travel advisories, which cover at the moment something in the order of 140 countries.

From time to time when there are special events—for example, ANZAC Day at Gallipoli—we may decide it is appropriate that, where we know that large numbers of Australians are going to be in one place at a given time and there might be some form of security risk, we issue a specific bulletin or advisory going to that specific event. Usually, our advisories are country specific rather than event specific but increasingly, as events of this sort occur—whether they be the Olympic Games or Anzac Day or the Bali commemoration coming up in another month—we work very closely with ASIO and with others to ensure that our public consular advisory is spot-on.

Ms GRIERSON—When you have put an advisory warning out regarding a site or a destination, there has been controversy in terms of the warnings not translating into action further down the chain. What is your involvement in making sure airports or other authorities linked to aviation are responding appropriately to those warnings?

Mr Hutchesson—For example, if there is an advisory that suggests that in a particular country there might be the risk of attack at airports, hotels or bars or the like, we would certainly draw that advisory to the attention of the host government. It may well be, if judged appropriate at the operational level—at the policing level or the intelligence level—that it is not inconceivable that direct action led, obviously, by the host country might be taken on the ground to deal with a specific threat. But that would have to be led by the host country. We are not in a position to intervene to nip attacks in the bud where they are not on our soil, obviously.

Ms GRIERSON—What is the process for an airline which knows there is that sort of warning restricting or encouraging people not to travel?

Mr Hutchesson—Our consular advisories are public documents, and I know that all of the airlines are aware of what we have to say. Of course, our consular advisories are based in part on classified threat assessments prepared by ASIO. I am aware that, from time to time, ASIO will have direct discussions with the airlines if there are particular issues of concern. But that is really a matter for ASIO.

Ms GRIERSON—It is for other agencies. Thank you.

CHAIRMAN—I have one last question, which goes back to biometrics and facial recognition chips. How can you stop someone reprogramming a chip or replacing the chip with another which matches the passenger?

Mr Nash—That is a very complicated issue, and it is one that we have not worked through entirely as yet. There are a couple of issues there. One is the security of the chip itself. Of course, the chip that we ultimately choose to put into our passport will have to have all the international certifications in relation to security requirements. That is the first thing. The second thing is what we call PKI—public key infrastructure—which is the ability to actually write to that chip and to access the information on that chip. Obviously a country would want to write to its own chips and would want both keys—one to write and one to access. Other countries, which of course ultimately would want to access the information on that chip at border control points, would require the access key. This raises a significant issue in terms of international security of keys and whether or not there is a need for an international repository of keys. The possibility at the moment is that such a repository could be established in the International Civil Aviation Organisation.

CHAIRMAN—I have read some information which has just come to my attention—an article on the wire from the *Sydney Morning Herald* about the theft of the Customs computers at Sydney airport. Is PKI enough if people can walk into secure environments and steal the computers that hold the keys?

Mr Nash—In our case we believe it will be. As I say, it is yet to be worked through. This is very similar to the technology that is used by banks to enable us to use our cards in various banks despite the fact that they might have been issued by another bank. We are talking very closely to and have had a lot of consultation with organisations within the commercial field, such as banks, about how this might work. The Americans and others are also working on it. It is obviously of major concern to us. We would not recommend implementation of biometrics until we have had this issue thoroughly resolved.

CHAIRMAN—You have not really addressed the issue, though. If somebody goes in and steals a server or part of the mainframe and has access to all the information on it and it contains the keys and, in fact, the code, how secure is your system then? It is not, is it?

Mr Nash—Our databases and all of our transmissions are done on national secure networks, and so—

CHAIRMAN—But how secure are they if somebody steals the machine? I do not think you understand: if the hardware is gone, your secure system does not exist anymore.

Mr Nash—No, I do understand the question. In our case, the levels of protection that we have for such machinery are such that we do not consider that it is at risk.

Ms GRIERSON—Would there be data there that, should it be taken and misused, would compromise the privacy of lots of individuals?

Mr Nash—I guess that brings me back to the same point: we do not believe it would be possible for other people to access it. There are certainly major privacy considerations involved in protecting the data that belongs to individuals. There is no doubt about that. It is kept on national secure databases and it is transmitted across national secure lines.

Ms GRIERSON—I guess the public would really want to know that the information that you may store, which contains their whole identity in some ways, is not able to be penetrated by someone else and then misused, taken over et cetera. When we know whole servers have been taken—not just a piece of hardware, but servers that have lots of data on them—then we would be very concerned. I would have thought you would be very concerned too, because that sort of equipment is going to be located outside your control in many ways. If you implement that sort of technology you will be dependent on the security of other people and the security provided on other sites. Is that a concern to you, and how would you respond to that?

Mr Nash—What we are proposing to implement in relation to biometrics is to simply store the same information we store now but do it in a slightly different manner. The security considerations there are really no different to the security considerations at present, and we are quite confident that the data we have at present is protected. The issue that we need to be particularly careful about concerns the information which will now be stored on a chip in the document. We need to ensure that those people who do not have the authority to access it are denied such access. We do that through, put simply, a form of encryption.

CHAIRMAN—That is what I asked you about before.

Mr Nash—That is correct.

CHAIRMAN—If the computer that is doing the encryption is stolen, of what value is this secure system? You say, 'Oh no, it is still secure.' How could it be? We do not have an Enigma machine doing encryption anymore, do we?

Mr Nash—No.

CHAIRMAN—It is a computer doing the encryption, is it not?

Mr Nash—Yes, it is.

CHAIRMAN—If I steal the computer that is encrypting all your data, how secure is your data, passwords, codes or anything? I would have thought not at all.

Mr Nash—This data will be protected to the extent that it has always been protected.

CHAIRMAN—That is not the answer to the question. If I steal the computer that is doing the encryption, how is your data secure? I now own the encrypter and all the codes; you do not.

Mr Nash—I would argue that you will not be able to get them.

CHAIRMAN—I would have argued that nobody would be able to steal Customs computers, but we are about to find out about that, aren't we?

Mr Nash—That is right. That is an issue for Customs, of course. I am not aware of what level of security Customs has in relation to that equipment, but I am very aware of the level of security that we have, and it is very high.

CHAIRMAN—Are you telling me it is not possible for anyone to gain access? The people who did the job, to use the vernacular, evidently pretended to be private sector contractors to gain access. They used false names, false addresses and false signatures, and they gained access. Are you telling me that no private sector contractors work on your computer systems?

Mr Nash—A large number of private sector contractors work on our systems, but these people are all vetted, and we are very careful about who we allow to enter our secure premises.

CHAIRMAN—I suspect Customs would also tell us that they are very careful about who they allow into their premises. My level of confidence is somewhat shaken at the moment. Thank you very much for coming. If we have further questions, would you mind if we put them to you in writing to negate having you come back and appear before the committee again?

Mr Nash—Not at all.

CHAIRMAN—Thank you once again for coming and for your submission.

[10.22 a.m.]

FREW, Mr Todd, Assistant Secretary, Entry Branch, Department of Immigration and Multicultural and Indigenous Affairs

HANNA, Mr Graham Wayne, Director, Air and Seaports Policy Section, Entry Policy and Systems Branch, Department of Immigration and Multicultural and Indigenous Affairs

McMAHON, Mr Vincent, Executive Coordinator, Border Control and Compliance Division, Department of Immigration and Multicultural and Indigenous Affairs

WILLIAMS, Mr Jim Robert, Assistant Secretary, Unauthorised Arrivals and Detention Operations, Department of Immigration and Multicultural and Indigenous Affairs

CHAIRMAN—Welcome. I realise that you are not directly responsible for aviation security, but indirectly you certainly have an important role to play, in that if the wrong people get in then we could have catastrophic results, and if we do not know who is here and they operate inappropriately I suspect we could have the same sorts of scenarios as occurred on September 11. In your submission, you said:

DIMIA works closely with ... other agencies to protect Australia's borders by maintaining effective screening of travellers. This occurs at all stages from visa process from application to arrival in Australia and by maintaining records of people's movements in and out of Australia.

How good are those records?

Mr McMahon—They are of a quite high quality. We always have some data issues with any system. Before the person arrives we know who they are, except in some very limited circumstances; they have already had a visa, so we have got a visa record of them. That is matched with the movement record as they board the aircraft. They are cleared through the border and it is clicked off on our system to show that they have entered the country; and when they leave the country their record is recorded. That is why we are one of the very few countries in the world—possibly the only country in the world—which can actually computer-generate a list of overstayers.

CHAIRMAN—You would be aware of the report on the ABC this morning, which has been followed up by a report online by the *Sydney Morning Herald*, about the theft from Sydney airport of two Customs computers—two big servers. Are you confident that you have no information on those systems, which are no longer in our possession?

Mr McMahon—Actually, I have not heard that, so I do not know what has happened.

CHAIRMAN—Evidently, on the night of Wednesday, 27 August, two men dressed as computer technicians and carrying tool bags entered the cargo processing and intelligence centre at Sydney airport and, some hours later, walked out with two huge mainframe servers. I would

have thought that Customs and the AFP ought to have let you know. If everybody is in the loop on sharing information regarding aviation security, I would have thought you should know.

Mr McMahon—I have not actually been at work this morning, so the issue may have been raised.

CHAIRMAN—It was the 27th. Today is the 6th.

Mr McMahon—Yes, I am surprised I have not heard that. Whether or not there is any of our data on those servers is an issue. I would expect, had there been any of our data on those servers, we would have been advised.

CHAIRMAN—Do any of your colleagues have any information?

Mr Frew—Mr Chairman, I heard it on *AM* this morning. That was the first time I had heard it. I have not had a lot of time this morning to pursue it further. I did take some comfort from the fact that it was in the cargo intelligence area.

Mr JOHN COBB—Why did you take comfort from that?

Mr Frew—I am assuming—which I realise is a dangerous thing to do—that our data is not in those computers in those areas; but I will know later on today.

CHAIRMAN—So you are highly confident of the security and the accuracy of your records regarding people. You say that you know all the overstayers. You might refresh my memory. When we did an inquiry into Coastwatch a couple of years ago, I recall—which I think was some comfort to the committee—that there are, at any one time, 30,000 individuals—

Mr McMahon—About 60,000 overstayers.

CHAIRMAN—I always get it wrong. Anyway, at any one time there are approximately 60,000 individuals in Australia who should not be here, for one reason or another, and every year we export 30,000; and every year another 30,000 arrive on the books. Is that about right?

Mr McMahon—We remove around 14,000 people a year at the moment. I would not say that we are absolutely delighted with all our records and that there is no scope for error. The point I was making is that we are probably one of the only countries in the world that can generate one of those lists in the first place. There is virtually no country which electronically records both entry and exit in a way that can compare the two sets of records to generate it. We do a lot of research around our overstayers; and we do generate names and we do generate follow-ups in respect of that data. Our APP system—advance passenger processing system—was the only system in the world, until New Zealand adopted a very similar system in recent weeks, which put a step in between the passengers submitting themselves at an overseas port and their flight to Australia. In other countries, they collect advance passenger information, but that is exactly what it is: it is information coming down the line. If we get a match of some description at the point of boarding, we have the choice of saying yes or no to that person being boarded. We do refuse boardings.

CHAIRMAN—You are, of course, familiar with the tests going on at the moment in biometrics—the facial recognition chips—with Qantas staff. What is your view of how that is progressing?

Mr McMahon—It is extremely interesting technology. It offers scope for both economy and increased accuracy in the recognition of people. It is early days in many respects. They have done a trial on a certain group of people. One of the big issues in facial recognition is the question of enrolment—that is, how do you get images into your database to make the comparison with the person coming through? Clearly, that is resolved to a large degree in the Australian context if you have a biometric in the passport; but, of course, more broadly most people do not have such a biometric in their passport. It is a very useful technology. It has got the potential to significantly increase the security around the border, but we have got a little way to go on it.

CHAIRMAN—Under your memorandum of understanding with ACS, all persons who enter or depart Australia must be confirmed visually by an ACS officer as the same person whose photograph appears in the presented travel document.

Mr McMahon—Correct.

CHAIRMAN—Have you audited that process? What per cent of the time do we get it right? What is the failure rate? Do not tell me it is zero, because we know that is not right.

Mr McMahon—I can answer that in two ways. We expect that process to take place on 100 per cent of the occasions. We have made our position clear on this with Customs, and Customs have accepted that view. Our people on the secondary line will walk along the primary line to satisfy themselves that in fact that facial check is taking place. The very difficult part of your question is: how would you know when you have failed? There is some research saying that people are not particularly good at recognising the photographs of like people, vis-a-vis a face before them. You could not ever conclude conclusively, I do not think, that a person consciously looking at a face would get it right on 100 per cent of occasions.

Ms GRIERSON—You have talked about your overstayers database—it is excellent that we do have that—and you have said that you have done some research on that. What are the common features of overstayers? Is there an age factor, a location factor, a skill factor or an ethnic factor? Who overstays the most?

Mr McMahon—That is a very difficult question to answer. Can I just take one step back from that for a second to explain the way our systems work? We have varying levels of scrutiny of people from overseas posts when they make application. We also have varying levels of eligibility about what people can apply for. For example, a person from a country at risk may not be able to apply for a particular form of student visa. Over time, as people of a particular nationality have overstayed, we have tried to change the visa regime as it applies to that particular nationality. That is built into the Migration Act.

I can give you an example of the way it works and why it is a changing position. We had a very significant overstay rate with people from, for example, the People's Republic of China. We then had fairly significant changes in the level of documentation that they required and we also

entered into new arrangements for the way people could enter Australia as visitors. We put the responsibility back on the travel agents in the People's Republic of China to verify passengers, and if they could not maintain a certain rate of overstayers—in other words, keeping that rate of overstayers—we suspended them or struck them off the list. So within about three years the PRC went from being a very obvious overstayer country to being a country with an overstayer level that is quite comparable to that of a number of other countries.

Similarly, in respect of things like electronic visas and all those sorts of things, eligibility will change. We find that, depending on visa class, people perform differently in respect of overstay. You have to work through each visa class to establish the characteristics. For example, if you look at the issue of sex trafficking and people working illegally in the sex industry, you find that one in two people found working illegally in that industry are Thai women aged between 20 and 30. Similarly, if you look at students, you find that the overstay rate is probably going to be high for people from the Indian subcontinent and, potentially, China. If you look at some of the visitor overstay rates, you find that the highest numbers of overstayers are the high-volume people from the UK et cetera but that the percentage increases are from countries in our immediate vicinity, like the Pacific.

Ms GRIERSON—I ask about that because it is important that you know the patterns of overstaying so that if you see changes you can respond to them. Obviously, there is a system in place. There is no process for acting on overstayers, is there? You do not know where they are once they overstay.

Mr McMahon—You are quite correct. Essentially, when you look at people before they come, we can treat them as a group and apply rules and levels of scrutiny.

Ms GRIERSON—And assess the risks there.

Mr McMahon—Once they overstay, we tend not to look at individuals but to more broadly take a view of where they are most likely to be working. We tend to look for illegal workers in the retail industry, the restaurant industry, on sites, low-skill type stuff. Although the system of dob-ins is very crude, it is extremely effective and a very important source of our information. One in two dob-ins leads to some substantive action resulting in a visa regularisation issue arising.

Ms GRIERSON—The reason for this inquiry into aviation security is that there have been two reports done by the Audit Office where they were not satisfied, and we were not satisfied, that there has been enough improvement in aviation security generally. The reference that the chairman made to the theft of the servers was not just from a cargo area but from the top security mainframe room located in the airport. It was that central and that important a location; it was obviously the most sensitive place, because that is where the sensitive data is. Since the 1998-99 audit, we would have hoped that there would have been significant and observable improvements in aviation security. You operate in airport environments—or your officers do. Could you comment on your observations in those environments of any improvements, the areas you have seen that have obviously been tightened and those that perhaps need concentrating on?

Mr McMahon—From our point of view, the chairman's summary at the beginning of this hearing was very relevant. We know that if people can move through our borders without our

knowing then that is a very significant concern for aviation security—and that is where we have placed our focus. The advance passenger processing system has been a primary area of our focus; we want to know who is entering the country. Since February this year, it has been compulsory for most passengers and crews coming to Australia to be advance passenger cleared. There are further milestones coming forward in legislation which we believe are extremely important in providing the wider coverage that we need to be satisfied. From 1 January, for example, people in transit lounges, which are an area of concern, will also have to be advance passenger cleared, as well as people in passenger ships—in other words, we are putting the emphasis back across to the port a little bit. We will have much more comprehensive view. Basically at the moment we have a movement record for something like 94 per cent of all people coming to Australia before they reach the country. We are now closing down quite rapidly on the remainder.

Ms GRIERSON—Can I just interrupt you there. I am confident that you are confident that your pre-arrival and screening systems are good, and therefore you believe that you have fairly good control over who comes in and you know who they are. My problem is that, when they come through an airport, it rests on the people working in that airport to use the identification systems, whether it is a visa or a passport et cetera, so you are relying on the culture that exists within the airports to take security, identity and people's right to be here very seriously. Do you think that, on the ground, that is operating the same as it always has, or do you think it has improved? Do you think there is a more rigorous approach not to the information they have—because you have answered that very thoroughly—but to dealing with that information? What are your impressions? Have you scanned that in any way? Do your workers comment on that; do they have feedback on that? Do you have any feedback on failures—are they increasing, are the wrong people getting through? You said people do not recognise faces as well. That is right; they let people through after just looking at the photograph. Often there is a total mismatch, but the person still goes through. Do you have any evidence of the improved security and compliance you would anticipate?

Mr McMahon—I will leave it open for other people to comment on this as well. First of all, I would observe—and it is possibly counterintuitive—that the level of interceptions at the border is actually dropping. That to us is not a concern but a verification that our systems are working, because we are screening a lot of people before they come in—before they reach the border. I am very satisfied with the seriousness that Customs, as our agents, are applying to the identification of a person. That is something which is extremely important to us and a shared concern. It is an understanding of some of the limitations of visual screening which has pushed Customs—with our support—towards things like SmartGate. Customs are also bringing forward a fraudulent document detection system at the border, which is a multi-layered system of document examination and which we hope will work very effectively. By putting it under their screens, it does the ultraviolet test and a whole series of other tests in one go. We are working closely with Customs on that. One of our concerns is that it may throw up a lot more work, but if it is throwing up work that is warranted then we would welcome that.

Ms GRIERSON—Regarding that fraudulent travel document investigation process, I suppose we have all seen drivers licences that can be printed off onto a piece of plastic from a computer by almost anybody, and we have seen whole batches of passports turning up that have been illegally produced. I guess we are all familiar with the ATM devices that are accessing information as a card is processed, and then we hear of the biometric identifier type technology.

Most of us would say, and would predict accurately, that any new technology would be open to fraudulent use and penetration by people you did not want it penetrated by. That would suggest that the intelligence you rely on is probably more important than anything else.

So there are going to be some breaches of security in relying on identification. However, good intelligence exchange and the communication of it to the right people would be the best way, perhaps, to override some of those concerns. How is intelligence shared when you have any high-risk notifications or any belief that there are people trying to enter this country illegally? How is the process shared? Obviously, we are particularly looking at people who may want to come through airports. How is it responded to? Has the system changed since September 11? What do you think of the state of intelligence exchange in terms of it being a failsafe system?

Mr McMahon—In terms of the description of what happens, which is fundamental to this, we have a movements alert system and part of that information—the alerts themselves—is provided to us by security organisations.

Ms GRIERSON—Australian and international?

Mr McMahon—The security organisations may receive their information from a number of sources, but it is only fed through in that one area. When there is a hit on that, it is not information which is available to the department of immigration, but ASIO, for example, would be immediately alerted that a hit has taken place. We would then require from them an indication of whether or not they would want us to board the person or issue or not issue a visa. The mechanics around that decision are obviously not open to us; we basically—

Ms GRIERSON—You just respond to it.

Mr McMahon—We respond to that instruction. Consequently, I think it is a system that works extremely well for the security organisations, because they get so much warning of it. Of course, nothing will ever warn us about a person who is travelling fraudulently under a document—often people can actually buy legitimate documents, which is always a potential issue. The other thing which was very important from our point of view in the explicit response to September 11 was the significant increase in the level of airport liaison officers overseas. Until a few years ago, airport liaison officers were something we did not use all that extensively.

Ms GRIERSON—Who employs those people?

Mr McMahon—We do. We have 16 airport liaison officers, and they are basically spread in an arc starting from Nadi, working their way up to the Philippines and across to Taipei and Korea and then down across Bangkok—

Ms GRIERSON—So they are concentrated on our Asia-Pacific region?

Mr McMahon—At the gateways to our regions. They have a number of purposes. One of them is to increase the level of training to—

Ms GRIERSON—Yes, for security.

Mr McMahon—airlines et cetera. But they also look at the documents of people moving around in the regions. For example, in the last year—

Ms GRIERSON—How can they do that?

Mr McMahon—Sorry—in the region to Australia. Also, they actually work collectively with other countries' airport liaison officers, particularly in Bangkok, which is a major gateway. For example, nearly 300 people were stopped from entering Australia from a visual look at the documents, and something like 1,500 people were stopped from moving within our region, which may have included subsequent travel to Australia. With the fact that we have these causes and avoidance, people know it is very difficult to come to Australia with bodgie documents et cetera.

Ms GRIERSON—You said there were 16 officers. Has that number increased since September 11?

Mr McMahon—Yes, it has. My recollection is that prior to that we had something like five overseas. I might be corrected on the facts here, but we certainly have been increasing that.

Ms GRIERSON—So it is significant.

Mr McMahon—It was a specific response in the Prime Minister's statement—that there be an increase in the number of airport liaison officers.

Ms GRIERSON—As you have said, they liaise with other similar international authorities for information.

Mr McMahon—Yes. In Bangkok I think a number of countries are air side. In a lot of other countries we are the only airport liaison officers there.

Ms GRIERSON—Do they also respond to ASIO advice in terms of any possible movements they would be tracking, or do you not have access to that information?

Mr McMahon—The airport liaison officers play a slightly different role. They have no authority at all, because they are operating in other countries. In respect of the visa issue, the ASIO advice should have been picked up, and so that should have happened before that stage. What they look at are the actual passengers and the documentation they are carrying.

Ms GRIERSON—That is probably much more informed intelligence than I would have anticipated. What would be the other key or most important intelligence exchange that happens for DIMIA?

Mr McMahon—We have established and grown in the last two to three years very significant in-house intelligence, and we coordinate more broadly with other agencies in respect of unauthorised boat movements and people-smuggling networks. Some people-smuggling networks have the potential—and we have seen it—to move, for example, from a boat to a plane. In other words, when looking at passengers, they consider whether they move them by boat or plane. They may move them by boat to a third location—for example, PNG—and then

move them on from there. We have very significant intelligence sharing with those agencies. We have very close links with the AFP. We are looking at migration agents in some cases as being a common source of assisting with the illegal movement of people. We established an internal task force quite recently which is explicitly looking at targeting migration.

Ms GRIERSON—Are you suggesting that there is the possibility of migration agents being easily corrupted to assist with or facilitate illegal travel?

Mr McMahon—Yes, but I must say 'some' migration agents. Most of them operate as legitimate businesses and provide a valuable role. But certainly, for example, with the sex trafficking industry, when we go into brothels we often find that the women there are on bridging visas. Bridging visas are issued when there is a substantive application and invariably the substantive application is a protection visa. If you ask the person involved about the nature of their protection visa, they often cannot give you any details; sometimes they do not even know that a protection visa has been lodged. Then you have to look back to the migration agents, and you will find that there are some migration agents who have a zero success rate in respect of all of the applications they have submitted on behalf of their clients.

Ms GRIERSON—If I have travelled to and from Australia many times and have had many visas issued et cetera, where would all that information be stored?

Mr McMahon—Information is stored in our systems; we could pull out very rapidly the movement records of any person who has been cleared through an airport.

Ms GRIERSON—It is on your computer systems. Would you archive things, just like everybody else does? Do you keep computer records for a certain period? Do you have any protocols for doing that?

Mr McMahon—We have protocols and records; I actually cannot speak definitively about those. But yes, we do back up our systems. We have outsourced arrangements, and issues, including those of security, have been put to those outsourced arrangements. Unfortunately I am not the person to answer that question in detail.

Ms GRIERSON—We are more sensitive to the integrity of our computer systems today.

Mr Frew—Mr Chairman, perhaps I might respond to the question you asked earlier about the theft of the Customs servers from Sydney airport. We have received advice this morning that there is no immigration data on the stolen servers. I suppose the question remains: why did we hear of it on *AM* this morning, as did you, rather than hearing of it from Customs?

CHAIRMAN—I will be asking them that very shortly.

Mr Frew—Perhaps when I am not in this room I will ask them that question.

CHAIRMAN—I can assure you that I will be asking them that on the public record very shortly.

Mr Frew—And your request will have far more authority than mine.

CHAIRMAN—That is only because we have an act of parliament that defines us and we have been hanging around for 90 years—not us personally but the committee.

Mr JOHN COBB—Mr McMahon, what do the records and history show as the preferred method of entry by people who are obviously of concern to us at a time like this? It would hardly be immigration. I would imagine that that would take too long. Is it straight out illegal immigration? Is it by tourist visas? Is it business visas? How do they normally try to get in?

Mr McMahon—I will preface my comments by saying that we have a silent partner in respect of security type issues. We would know whether there is a hit, but we do not know anything that happens after that until we are told by the security organisation what we should be doing about it, which is most often a rejection. But the major source of overstayers in Australia, and it is not surprising really, is tourist visas, because overwhelmingly they are on that visa.

Mr JOHN COBB—I am not too worried about overstayers who just want to enjoy our good climate for a while; I mean people about whom we are worried. What does history show us as the way they attempt to get in?

Mr McMahon—As I said, we are not in a position to do that sort of analysis in respect of security type issues. Most of the hits we have on our own system come about because the people have been in the country before and overstayed, because they have a debt to the Commonwealth that they need to repay or because there are health concerns around them. In respect of the people who are not hits but groups, as I indicated before, we tend to understand the nature of the level of overstayers in respect of the categories.

Mr JOHN COBB—I will come back to it another way. I am not sure to whom this question should be addressed, but could Mr Frew, Mr Williams or whoever it might be give us a brief overview of how you cooperate with DOTARS, DFAT and the AFP in terms of security at airports? How do you cooperate with them? Do you have regular meetings? Whether they be formal or informal, how do you do that?

Mr McMahon—We do have meetings at the airports where the agencies come together.

Mr Hanna—There is a regular meeting every three months between the deputy secretary of Immigration and the equivalent in the AFP. There are also regular local meetings held by the DIMIA airport inspectors at each of the international airports. In some airports—at the high-traffic airports—that is as frequently as fortnightly. That is increased for particular events or if the security is heightened for any particular reason, and there is quite a high level of cooperation there.

CHAIRMAN—Don't you have a MOU with Customs?

Mr Hanna—We certainly do have a MOU with Customs.

CHAIRMAN—Don't ever neglect to remind us of that.

Mr JOHN COBB—In that case, do you also have one with DOTARS?

Mr McMahon—I do not believe we have a MOU with DOTARS. We do have one with the AFP. But the MOUs go to particular issues. For example, the one with the AFP is about how we handle cases between us.

Mr JOHN COBB—Do you have a physical presence at every international airport in Australia?

Mr McMahon—We do.

Mr JOHN COBB—Does every single passenger coming into Australia go through your screen?

Mr McMahon—Yes, they do. Sorry, are we talking about aviation passengers now?

Mr JOHN COBB—We are.

Mr McMahon—Yes.

Mr JOHN COBB—The advance passenger processing system and MAL, the movement alert system—I like that name—sound very good. How do you work in with DOTARS in terms of screening et cetera? If they are responsible for security, do they work those systems for you in airports, or do you do it yourselves?

Mr McMahon—The way it works is that our mainframes talk to the Customs mainframe.

Mr JOHN COBB—So you actually work through the Customs mainframe?

Mr McMahon—Yes, we do. Essentially, there is a system called PACE, which is the Passenger Analysis Clearance and Evaluation system. That is the border system of Customs. Our mainframe talks to that system. Basically, there is an interface between the two of them. We download information to it. For example, as we update our MAL records, it gets copies of those MAL records for checking out the border and, as a person moves through the border, it registers that movement and passes the information back to us. Effectively, we talk. We do have varying relationships with DOTARS, but in respect of security, like the physical security aspects, you could regard us as a client of theirs. In other words, they create the environment within which we operate. Of course, we would want to be alerted to a particular security instance if that had implications for us, but I suppose in some ways, except where the passenger is involved, it is very much like having guards in front of Parliament House—that system that allows you to operate within here.

Mr JOHN COBB—I hope it works better than this one. You have an invidious job, and by and large you do it fairly well. However, in terms of cooperation and certainly in terms of what we are talking about now—airport security or, I guess, general security—are there areas that you think could be improved with cooperation between you, the Federal Police, DFAT and DOTARS? Are you happy with the way it is happening now, or do you believe it could be improved?

Mr McMahon—I do not think we have formed a formal view on that. Some issues have been raised in respect of DOTARS and, in some places, the way in which our staff are screened as they go in. If there is a back entrance—

Mr JOHN COBB—Do you mean your staff or their staff?

Mr McMahon—Our staff are screened. Customs have a similar concern regarding the fact that, once the line is drawn at a barrier, if you come through the front of it there is no regard for whether you are an official working in the airport or not. That is one of the minor bugbears which is being discussed within government regarding how you deal with that type of issue. Other than that, as I said, in respect of physical security we see ourselves more as a client. We have only had concerns about physical security where people are in our control and we have to deal with them ourselves. For example, we did an analysis of all other airports in respect of the way in which we might hold somebody in an airport and found that they did not meet the normal OH&S concerns in those circumstances. For example, an angry client could potentially break the glass and use it. We went through and fixed our own security issues through that checking, using security organisation advice.

Mr JOHN COBB—Are we cooperating with our APEC neighbours pretty well? Given our recent history and one thing and another—and especially the current state of affairs—are you reasonably happy with the way we are getting on with our neighbours in trying to determine the immigration issue and the records?

Mr McMahon—Extremely happy, actually. The one thing that Australia was very keen on was promoting advance passenger information. It was eventually taken up within the APEC context. There was a pathfinder initiative there and effectively what that pathfinder initiative did was create a pool of funding in which various countries would be given the assistance of APEC to develop advance passenger information systems. Australia, in fact, is the country which is actually providing all the technical support. We carried out a full survey and analysis for Thailand and handed that to the Thai government through APEC. We have also done the same in respect of other countries, such as the Philippines and Indonesia. It seems to us to be very much in our interests for regional border agencies to work more effectively. That is what we have been promoting.

Mr JOHN COBB—I could not agree more.

CHAIRMAN—I have one last very brief question. You have been provided with an exposure draft of the aviation transport security regulations recently circulated by DOTARS. Do you have any views about those regulations that you are willing to share with this committee?

Mr McMahon—Yes. The issue for us is that to some degree those security regulations reflect the view of the industry and some of the views of the industry have also been reflected in the submission to you from BARA. Essentially, the thinking around it goes like this: people in custody are people of concern. Therefore, if they go onto an aircraft they are potentially a person who is going to jeopardise security.

However, we do not regard people in immigration detention in the same way law enforcement does. Detention in an immigration context is administrative detention around regularising status.

With some of the people who come to our notice, of the 14,000 people who leave, over 10,000 are what we call 'monitored' or 'supervised' departures. They could be a backpacker who has overstayed by a day. No-one can claim that they are a dangerous person. It may well be that, because we could not be confident they would not run away again, we have taken them in overnight and we have taken them to the airport the following morning.

The way in which the regulations have been constructed would have everyone who we have an interest in, basically—in terms of leaving after overstaying—requiring a security assessment. That would present a minor bill of about $100 million a year to us. Importantly, it does not actually reflect the underlying security issues involved. When people are in detention, an assessment is done and if the person is a risk then we have arrangements with the airlines to provide escorts and a risk assessment to the airlines. So we have been very cooperative on that. But we would resist treating people who are simply leaving the country as security risks.

Ms GRIERSON—Briefly, I want to know whether you monitor aircraft crew and cabin and flight crew that come from within the airports?

Mr McMahon—We do now, yes. They are now being brought within the advance passenger processing from 1 January.

Ms GRIERSON—From next or last 1 January?

Mr McMahon—From January next.

Ms GRIERSON—From 2004?

Mr McMahon—Yes. Essentially, the way the APP works is that it checks against the visa. They do not have a normal visa because they are on a special purpose visa, so we are creating a crew travel record for them. They will have to register. We will do the checks against that and then they will basically move through the airports on the individual occasions under the same special purpose visa arrangements.

Ms GRIERSON—So that is a significant change and a measure that has arisen from the security threat?

Mr McMahon—Yes. It is the same on the marine side with the checking of crew. Very importantly for us, we have refused to accept—I do not know whether that is the right terminology—the international mariners documents. We want a passport and mariners documents—the passport for the identity and the mariners document to say what ship the person is actually moving on. So we are tightening up on the maritime side as well.

CHAIRMAN—Thank you very much, gentlemen. We appreciate your submission and your attendance. If we have further questions you will not mind if we send them to you in writing?

Mr Frew—No.

CHAIRMAN—Thank you. We will be interested, Mr Frew, in the outcome of your discussions.

Mr Frew—As I will be interested in yours, Mr Chairman.

CHAIRMAN—Just watch the box.

[11.11 a.m.]

KELLY, Ms Patricia, Head, Tourism Division, Department of Industry, Tourism and Resources

MURPHY, Ms Janet Anne, General Manager, Market Access Group, Tourism Division, Department of Industry, Tourism and Resources

CHAIRMAN—Welcome. I understand that you have not provided a submission. Do you have a brief opening statement, or should we just ask you our penetrating questions?

Ms Kelly—We do have a brief opening statement.

CHAIRMAN—Is it very brief?

Ms Kelly—It is fairly brief.

CHAIRMAN—Very brief?

Ms Kelly—I will make it very brief.

CHAIRMAN—Please. We have a special guest coming in a few minutes, and it is critical that we get to that issue.

Ms Kelly—Okay. I just wanted to highlight a few points for the committee, as we did not put in a submission. The first point I want to highlight is the high reliance of our tourism market on air travel, due to our status as an island nation remote from most of our major tourist markets. In 2002, over 99 per cent of the 4.8 million tourists who came to Australia arrived by air. Domestic tourism also relies to a significant, but lesser, extent on air travel. The second point I would like to make is that the tourism industry makes a very important contribution to the Australian economy. It provides 4.5 per cent of our GDP, it employs six per cent of our work force, and it provides 11 per cent of our total exports. The third point I want to briefly refer to is the fact that the international environment for tourism has changed significantly since September 11 and following events, such as the Bali bombing. There has been a significant downturn in the tourism sector as a result of these events.

Forecasts for healthy growth in tourism have been revised down, and they are under further threat due to safety fears, due to issues such as terrorism and also developments such as Severe Acute Respiratory Syndrome. Aviation and national security are fundamental to maintaining Australia's image overseas as a safe and welcoming destination. The way in which security measures are implemented will also be important in maintaining Australia's friendly and efficient border screening procedures.

From a tourism perspective, one of the key planks in our overseas marketing of Australia and its continued popularity is its image as being safe, secure and friendly. The impact of a terrorist incident in Australia on our international tourism markets would be enormous. The tourism

industry therefore benefits significantly from measures Australia takes to enhance aviation security and broader national security. These measures contribute to consumer confidence and willingness to undertake the long-haul air travel required by most of our international visitors to get here.

Airports, and services provided at them, including border control, create the first and last impressions of Australia and, therefore, have a significant influence on our image. So, while border security is paramount, it is also important that facilitation of passengers remains efficient. We believe the performance of border agencies in this regard is generally very good. However, even small additional delays in processing can translate into significantly longer queues and inconvenience, so we need to continue to monitor this.

We want to draw the committee's attention to the fact that expected increases in tourist numbers in a heightened security environment would have implications into the future for effectively managing passenger flows at airports. The Tourism Forecasting Council projects that international visitor arrivals will increase from the current 4.8 million in 2002 to around 7.6 million in 2012, which is an average annual increase of 4.6 per cent—or 58 per cent in total. Managing these increases in a heightened aviation security environment, while maintaining an efficient and welcoming service at airports, will present challenges. Overall it is important that there is an appropriate balance between increased security and passenger convenience, and in this regard new technologies have a potential to play an important role in ensuring that increased security requirements at airports are met, as well as maintaining efficient and friendly processing of passengers.

Finally, the committee is aware that the government has set up an interdepartmental committee to review aviation security issues and report to government. The Department of Industry, Tourism and Resources is part of that committee. Our role is to assess and advise on the impact of any proposed changes or enhancements to aviation security on tourism. After consideration, ITR did not make a submission to this committee because we believed that, looking at the specific terms of reference, we did not have particular expertise on top of what our colleague departments could add, but we are very happy to provide any assistance we can to the committee with tourism information.

CHAIRMAN—You talked about the downturn in aviation from September 11, from 12 October and from SARS. Have you got any numbers you can attach to that?

Ms Kelly—Yes, we have. We believe the SARS events have been the primary cause of tourism numbers falling over the last seven months by around seven per cent. Following September 11, there was a very major impact. It is somewhat difficult to disentangle that impact from the collapse of Ansett, which happened on 14 September, but into September 2001 arrivals fell by 9.1 per cent, in October by 11.3 per cent and in November by 18.2 per cent. It is also important to note that the forecasts of tourism growth prior to the September 11 events had been around seven per cent a year over the next 10 years. Those have now been revised down to 4.6 per cent a year. So it is not only the actual fall on last year's numbers that we need to look at, but we had a quite well-developed forecast based on experience of significant growth and that significant growth has been greatly eroded.

CHAIRMAN—I realise that Ansett is a complicating factor in the equation, but my next question is: has any of that loss in the international tourism market resulted in an increase in the market in domestic travel on airlines?

Ms Kelly—It is quite hard to disentangle that.

CHAIRMAN—I bet it is!

Ms Kelly—Domestic tourism has had a fairly flat growth profile over the last five or six years. Anecdotally and from evidence in certain destinations, there is some evidence suggesting that there has been a switching from outbound tourism to domestic tourism. We have had quite good growth in 2002, with higher growth in domestic tourism than we have had in previous years. We believe that there is some effect, but it is hard to actually quantify what that effect is.

CHAIRMAN—I can understand that. The demise of Ansett did very much complicate the issue.

Ms Kelly—It did.

Ms Murphy—To add to that, if we are looking at the switching that occurred as a result of the Iraq war and the SARS epidemic, the figures show that outbound travel fell by almost 20 per cent over that period, while domestic tourism increased very marginally. So there is some evidence that there was certainly a degree of switching.

CHAIRMAN—I do not know how you are going to, or if you will, answer my next question. Certainly you would have seen the front page of the *Australian* yesterday. It is well recognised that we have freedom of the press and that we value that very greatly in our democratic society; it is very important to how we function. Would you have any qualitative or quantitative idea of how unhelpful the photograph of a SAM and a Qantas jet together on page 4 of yesterday's *Australian* would be to domestic and international tourism for Australia?

Ms Kelly—One of the things that we do not have a great deal of empirical evidence about is to what extent changes in aviation security have either positive or negative impacts on tourist perceptions. The Australian Tourist Commission do research in overseas markets on consumer perceptions of Australia, and they are looking at adding some questions to their surveys on perceptions about security. Our Bureau of Tourism Research, which is a Commonwealth-state tourism research body, carries out an international visitor survey. It surveys 20,000 international visitors in Australia each year. We are also seeking to put some questions on that survey about tourists' perceptions of aviation security. By those means we hope to get some empirical evidence about what the views of tourists are. We think that there are a couple of conflicting responses going on. On the one hand, it is reassuring to travellers to know that we are aware of security risks and that we are putting in place measures to minimise them. On the other hand, these measures might heighten tourists' awareness of risk, and they might lead to inconvenience for tourists. We think some conflicting responses are going on with tourists, and we are looking for some ways to measure them.

CHAIRMAN—I appreciate that that would be difficult. It seems to me that we, Singapore, Canada and, I think, Hong Kong were pretty open about the number of SARS cases and what

was happening. The initial response of the PRC was to try to pretend it did not exist. They woke up eventually, thank goodness. My feeling from anecdotal evidence is that tourism did better under the open environment than it did under the closed, 'pretend it is not happening' scenario. Do you agree with that? Do we have any idea about that?

Ms Kelly—I think it engenders confidence in people looking to travel to Australia that we are open about any problems we have and put in place measures to address them quickly.

CHAIRMAN—That is good.

Ms GRIERSON—I am particularly interested in the downturn you project and that it is real and continuing in terms of tourist travel to Australia. We are looking at the introduction of new security measures, which are quite costly and which obviously will be passed on to someone. I cannot see the airports carrying all the costs. I cannot see the government carrying all the costs. Obviously, passengers will be asked to carry some of the costs. Have you done any research, or do you have any views, on that impact? You have talked about the impact that the inconvenience of security is having on people's perceptions about travelling to Australia. What if they had to carry more cost because of aviation security and technology requirements?

Ms Kelly—We do not have any empirical evidence of the impact of cost, and the impact of cost is somewhat different on different segments of the market. So the business travellers are very time conscious but not so cost conscious, whereas leisure travellers, particularly backpacker type travellers, are very price sensitive. We know that it is a very competitive world market out there at the moment in terms of tourism as people try and rebuild their markets. On the other hand, if you look at the long-term real costs of air travel, you will see that over a period of about 10 or 20 years they have reduced—and they are one of the few things that have.

Ms GRIERSON—Regional airports particularly have escaped from many of the impositions of security in terms of the high cost of technology for security. Do you have any views on whether regional airports and regional travel could bear that cost?

Ms Kelly—Certainly the views of the industry that are put to us suggest that there would be difficulties with many regional airports meeting additional security costs. However, from the tourism point of view, we would point out that for domestic travel there is a much lower reliance on air travel. I think 76 per cent of travel by domestic travellers in Australia is by car and only 17 per cent is by air. There are some areas of Australia which are very dependent on air travel; Broome would be a good example.

Ms Murphy—Broome, Darwin, the Whitsundays, Hamilton Island and Cairns.

Ms Kelly—Cairns is a big airport, but some of those areas would be particularly hard hit. I think the impact would be patchy.

Ms GRIERSON—Has overseas charter to Australia been seriously affected or had it grown to a point where it was significant? Has it changed? Is it growing or is it diminishing? Do you have any information on charter flights to Australia?

Ms Kelly—It is not a huge sector of the market, but it is certainly one way of growing capacity and growing convenience, if you like. We have seen some new charter activity this year in the recovery from SARS in particular. We have seen charters out of Japan direct to Alice Springs and Cairns, which has been a welcome development. There are challenges in chartering to places like Alice Springs, which do not normally have the passenger processing facilities for international travellers and require both staff and equipment to be brought in specially—I think at a cost of around $10,000 per plane in those recent cases—to allow those charters to land at those places.

Ms GRIERSON—So there have been direct international charters into Alice Springs, and that means all the processes—such as customs and immigration—have to be put in place for that flight.

Ms Kelly—They have to be brought in specially, and that is paid for by the charter company—I think in this case it was Qantas.

Ms GRIERSON—So it was paid for by the company that chartered Qantas to fly the flights.

Ms Kelly—Yes. So if there are higher levels of requirements then those costs would become more expensive.

Ms GRIERSON—I do not know the situation at Alice Springs. Does it have the facilities to screen baggage and people coming through?

Ms Kelly—In the recent case, I believe that had to bring in X-ray equipment.

Ms Murphy—Alice Springs is not designated as an international airport so when an international flight comes into Alice Springs and the normal security arrangements had to be put in place they had to be brought in from Darwin or Adelaide in this particular case. For example, it does not actually have the X-ray facilities, the dogs or the personnel on site.

Ms GRIERSON—Have there been any other instances of airports being used that are not normally international airports?

Ms Kelly—There would have been, but I do not have the details of that.

Ms GRIERSON—Thank you for that information.

Ms Kelly—I would make the point that if we did increase security for domestic travel, it may mean that some of these airports would be more equipped for charters.

Ms Murphy—Coolangatta airport is a good example of an airport that put a lot of effort into growing charter traffic and now has far better facilities in place. So it can help grow an airport and a market.

Mr JOHN COBB—In your opening statement you mentioned, quite rightly, how important the tourist trade is to us. Did I understand you to say that, while obviously security is the number one thing and we have to be absolutely 100 per cent on it, you have some concerns about the

way we treat people coming in, or were you making the point that we need to reassure people? Do you have concerns about the way we are currently doing it? Were you making a point there?

Ms Kelly—Our view is that we currently do it fairly well by international standards but that even small changes, such as even a small additional delay in processing each passenger, can suddenly lead to very long queues. The point I was making was that in making any changes we need to monitor quite closely what the impact is on passenger processing and inconvenience.

Mr JOHN COBB—I am sure that, subject to all the procedures being met, we would all agree with that. You are not really pointing the finger; you are just saying it is something we need to be mindful of.

Ms Kelly—That is right.

Mr JOHN COBB—With most of the international airports outside the major cities, most of the passengers they get would be tourists. I am talking about, I guess, Townsville and Darwin. Most of the international passengers they get would be tourists rather than other travellers. I am talking about the regional international airports, in other words.

Ms Murphy—For the main ones—and Cairns is probably the best example—yes. That would certainly not be true for some of the smaller regional airports. For them, they are primarily only domestic travel in any event. But for the major regional airports, leisure travel would be the primary cause.

Mr JOHN COBB—I guess that was my point. But for Townsville and Cairns et cetera nearly all international passengers are tourists, as contrasted against what might come into Sydney or Melbourne, where far more international passengers are probably business orientated.

Ms Murphy—In fact, business travel classifies as tourism travel as well if it is a short-term stay. But yes: the difference is whether they are travelling for leisure purposes or to visit family and relatives, as opposed to primarily for business. Townsville and Cairns would certainly fall into that category.

Mr JOHN COBB—With the smaller airports, is the handling of people, from your point of view, better or worse than in the major ones?

Ms Kelly—Are you talking about—

Mr JOHN COBB—I am talking about tourists, I guess.

Ms Kelly—Are you talking about international—

Mr JOHN COBB—Yes, I am.

Ms Kelly—travellers coming into places like Coolangatta?

Mr JOHN COBB—Yes.

Ms Murphy—We really cannot comment on the relative—

Mr JOHN COBB—I am coming back to the point you made earlier: we have to be mindful that our reputation is at stake. It is second to security, of course. But I wondered whether there was a difference between the way it happens in the regional international airports as against the Sydneys and the Melbournes?

Ms Kelly—I think the procedures are fairly standard.

Ms Murphy—I would suggest that for some of those other regional airports there is less potential for passenger queuing than there might be, for example, in Sydney during the peak period in the mornings.

Ms Kelly—From time to time we get reports that there are particular problems at airports. That usually happens when the airport is having renovations or something is being changed and you suddenly find that you are getting reports out of Melbourne, for example, that there are problems with queues. But these things shift around. There does not seem to be a pattern in which we get particular complaints about regional or capital city airports.

Mr JOHN COBB—Thank you.

CHAIRMAN—There is some demand out there for increased screening at regional airports and smaller regional airports. Will you be playing a role in discussions between DOTARS and the AFP, and anybody else who is interested at a strategic level in security issues, to reflect whatever concerns you might have about any impact on tourism?

Ms Kelly—This is something that is being considered by the interdepartmental committee reviewing aviation security. We have a seat on that committee, yes.

CHAIRMAN—You have a seat on that committee?

Ms Kelly—Yes, we do.

CHAIRMAN—That is good. Do you have any memoranda of understanding with DOTARS or any of the other agencies that are involved in major issues in this inquiry?

Ms Kelly—We do not have memoranda of understanding but we are part of a number of committees.

Ms Murphy—For example, we are members of the National Passenger Processing Committee chaired by Customs. We have been on previous IDCs with the Transport on security issues. So we are generally fully engaged and part of the relevant discussions and the relevant standing committees that are set up to look at these issues.

CHAIRMAN—I know this is subjective and perhaps it goes to policy, which you will not answer, but would you have a view as to whether MOUs are useful in this sort of situation? Committees are committees are committees—there are lots of committees—but they do not set down in black and white what must occur between two consenting parties.

Ms Kelly—I think they can be useful to formalise arrangements, if that is necessary, between two bodies. To date, we certainly have not felt that we have been excluded from government discussions on passenger processing or aviation security issues.

CHAIRMAN—I am glad to hear that. We particularly like MOUs. We have a fascination with them, because they seem to get great outcomes. We observed that with Coastwatch. They are highly critical where a broad range of diverse agencies with diverse interests have to get together and work to make the system work. As I have said, if you were designing a system of border security, you would never have come up with what we have for Coastwatch but, since we came up with it, it is probably the best in the world. It is MOUs that make it work—that is, a lot of it anyway. Thank you very much; we appreciate your support. If we have any further questions we will put them to you in writing.

[11.38 a.m.]

FLOYD, Dr Robert Bruce, Leader, Program Development, Secure Australia Program, Commonwealth Scientific and Industrial Research Organisation

FULTON, Dr Neale Leslie, Principal Research Engineer, Commonwealth Scientific and Industrial Research Organisation

GIUGNI, Dr Stephen, Acting Director, Information and Communication Technology Research Centre, Commonwealth Scientific and Industrial Research Organisation

KING, Dr Warren Duncan, Executive Chair, Information Technology Manufacturing and Services Group, Commonwealth Scientific and Industrial Research Organisation

CHAIRMAN—Welcome. Thank you for your submission, which we have received. Do you have a brief opening statement, or may we proceed with our penetrating questions?

Dr King—Yes. Thank you for the opportunity to make a further statement in relation to our submission. Aviation security is a responsibility shared between government, the regulators and security agencies, private industry—that is, the airport and airport owners—the general public and the science and technology community. The role of the science and technology community is to provide technologies that prevent, detect or minimise the consequence of hazards and to identify technologies that, of themselves, could be a threat. Science and technology can assist in achieving the balance between civil liberties—that is, the privacy and freedom aspects—and security. We acknowledge that zero risk in the aviation industry is unrealistic. S&T can help to manage the residual risk such that it becomes an acceptable level of risk without significant erosion of civil liberties and prohibitive cost.

CSIRO has a strong history of contribution to aviation security and has many capabilities that could achieve further enhancement. The likelihood of security incidents could be reduced by better airspace modelling and enhanced personal identification systems. Neutron scanning technologies are currently being trialled for scanning air cargo in unit loading devices, ULDs, for the presence of explosives, firearms and other contraband. The consequence of airline attacks could be reduced by incorporating technologies to destroy microbial organisms as they pass through airconditioning systems and by the application of advances in material science to robust aircraft design. The above list of technologies should not be interpreted as evidence that airline security is inadequate, since we are in no position to make such an assessment, but as merely pointing out the opportunity for continual improvement through the application of new science and technology.

Airline security needs an effective mechanism for partnership with the S&T community, and I shall briefly illustrate with an example of partnership between the Australian Customs Service and CSIRO that has been very effective. Australian Customs identified the need and set the specific requirements for a fast and effective scanner for detecting contraband in ULDs, the unit loading devices. They then identified a CSIRO team that supports the mining industry as having a capability with the greatest potential to meet their specific requirements. The partnership, with

funding from Australian Customs and CSIRO, has now resulted in a laboratory prototype that is achieving the specifications required. The next phase is to establish a working scanner at a major Australian airport. Effective partnerships of this type can only work if agencies or companies responsible for aviation security have the prescience to correctly identify need or opportunity and the flexibility of funding to accommodate such exploratory devices.

Finally, it is perhaps worth emphasising the long period that can often take place between when a product is at the prototype stage in the laboratory and when it can be used routinely in external environments. Intervals of many years are not uncommon, so some of the technologies we have spoken about will not be available for some time. However, it seems likely to CSIRO that issues of aviation safety will be with us for many years to come, so research and development, even with its long lead times, still has a role to play in increasing that safety.

CHAIRMAN—Thank you very much. The CSIRO has been involved in biometrics. Could you tell us in layman's language how it is going to work?

Dr King—There are many facets of biometrics.

CHAIRMAN—In terms of passport security—the individual identification.

Dr Floyd—One of the exciting advances in the biometrics area is being able to combine that with the optical variable device technology, which is some of this anticounterfeiting stuff that goes with those glassy windows in the bank notes, where personal biological information is able to be encoded and encrypted. That is some of the technology that is being explored and looked at at the moment that certainly will make it very difficult for people to counterfeit or forge personal identification.

CHAIRMAN—How far away are we?

Dr Floyd—That is a good question.

CHAIRMAN—I know it is always difficult.

Dr Floyd—The bringing together of the biometrics side and the OVD technology, the optical variable device technology, is only just happening at the moment. I am afraid I could not answer exactly how long that is likely to take before the big product will come out at the end of that.

CHAIRMAN—No matter when, whether it was next year or in five years time, you would probably agree that it will take many years to survey the travelling population of the entire world?

Dr Floyd—The process is probably more about what kind of mechanism of identification system should be rolled out, and that is a policy issue more than a scientific one. I think that we can provide, within a number of years, the technology which would enable encrypted biometric data to be put into these OVDs.

CHAIRMAN—But can you do it so that it can be done quickly, simply and economically? That, as you well know, is very frequently the scientific and engineering challenge.

Dr Floyd—It certainly can be. The writing and the storing of the information can be done quite quickly and, I would say, cost effectively if this technology all pans out well. It is getting the information as to what you are putting in there which needs to be looked at.

CHAIRMAN—In your submission, you talk about risks associated with aviation security. You say, 'The main mechanisms of risk include baggage, freight, cargo and post'—that is dot point No. 1. Dot point No. 2 is 'on person' and dot point No. 3 is 'aircrafts themselves'. How come you wound up with baggage, freight, cargo and post being the first dot point?

Dr King—I am not sure that that was actually a priority system; I think that was just a list.

CHAIRMAN—That is why I wondered.

Mr JOHN COBB—It is the three issues, rather than an order—

Dr King—That is correct. I do not think there is any sense of prioritisation there.

CHAIRMAN—The context in which I ask is that most of the world's attention has been focused on passenger movement and trying to detect whether or not passengers carry weapons onto aeroplanes and/or put bombs or other weapons into aircraft holds which they might be able to activate. It seems to me that that is the greater risk. We have not paid as much attention to cargo as we have to people movement. Do you think that is a potential fault of the system?

Dr King—I am not sure it is a fault. Inevitably, any facet of a system which is seen to have an avenue for use will, I presume, be targeted at some stage. I see this at all times as a race between technologies that one part of society is trying to use against the other part, so at some stage it would seem possible that cargo will be targeted as a means of doing damage to aircraft.

CHAIRMAN—You talked about full-body scanners, capable of seeing through clothing and producing detailed images of bodies, now being trialled at airports. Doesn't that create a huge privacy issue?

Dr King—Of course it does. In fact, you cannot imagine that such technology would be brought into place without huge numbers of safeguards that would go along with the privacy issues. But, in the first instance, one can see some simplistic ways that you could do that. Sensitive areas could be removed automatically from images, et cetera, so that you could still have some capability whilst trying to avoid the worst aspects of the privacy issue.

Dr Giugni—One could imagine it being a secondary form of scanning rather than a primary mechanism that everyone goes through.

CHAIRMAN—I realise that you are all scientists. Me too—I actually have a degree in science. I do not know what that proves. Your submission does focus on technological issues—

Dr King—That is correct.

CHAIRMAN—But do you have a view or views on the human component of the security issue?

Dr King—I think it would be dangerous for us to have a view, quite honestly. We are representing an organisation and its technological aspects, and probably there are people who are far better qualified to talk about the human aspect of this than we are.

CHAIRMAN—But don't you think about motivation and risk when you think about how you might use technology that you know about, or that is being worked on, or that has the potential to help industry later? Don't you use that vision of what might come down the track? You have just told us that you might have some very strange things coming through aircraft ventilation systems that I had never thought about—in other words, new terrorist methods of operation. Don't you fast-forward?

Dr Floyd—I think the issues that you are raising are very important. One of them, which we made evident in our opening statement and which we will table, was that the engagement with the science and technology community is very important for identifying threat technologies—not just the technologies to overcome threats but what technologies might in fact be threats. We are very strongly of the opinion that there needs to be very good engagement between the science, engineering, technology community and those responsible for aviation security. We are also very aware that there is this balance required between security and civil liberties. The decision about how that balance is weighed it is not one for us to make but one for us to inform from a technological point of view.

CHAIRMAN—You would probably be aware that yesterday's *Australian* newspaper carried a banner article about SAMs and a photograph on page 4? with a Qantas jet aircraft and a missile in the same frame. I am not sure that that is horribly helpful but I believe in freedom of the press. Do any of you have any knowledge of these missiles, how complex they are to operate and whether we should consider that there is any domestic security threat in Australia from MANPADs or even how difficult it is to train people to use them? My understanding is that the last two attempts made—I believe they were in Turkey—failed because the people operating the system were not trained well enough to make it work properly.

Dr King—I do not think we have any knowledge at this table, and I would be surprised if anybody in CSIRO did. CSIRO does not do defence related work, which is where I would expect this particular research to fit the technologies. We have a number of technologies from time to time that have some application in the defence base, but we do not set out to actually do defence research.

CHAIRMAN—You are very good at over-the-horizon radar.

Dr King—To the best of my knowledge, that is really a DSTO technology, as opposed to a CSIRO technology.

CHAIRMAN—I thought you were very heavily involved.

Dr Fulton—We have navigation capability but not the operational capability that you are talking about.

CHAIRMAN—Fair enough. I accept that.

Dr Fulton—We understand the mass of navigation systems, but you are talking about how to operate such devices.

Dr Floyd—Another critical issue that comes out of your question is the place of the intelligence agencies in aviation security and also in that partnership with the science and technology community. We do not have, and probably should not have, access to the intelligence information which allows priorities to be set and, as a research agency, to work out where we should put our money and what the real threats are. We can look at vulnerabilities but we cannot look at threats, and that is why we need this kind of partnership of different parts of the aviation security area.

CHAIRMAN—Do you interact with DOTARS, with Customs, with Immigration and with the Australian Federal Police on the issues of the kind that we are discussing here?

Dr Floyd—Yes.

Dr King—I know of interactions with all of those agencies on various technologies.

Mr JOHN COBB—Do you have a formal role with DOTARS in advising them? I notice all the different technologies you are looking at, and you made comment on the different technologies for screening et cetera. Do you have a formal role in advising DOTARS and keeping them up to date?

Dr King—I am not aware of a formal relationship like that, but I am aware of interactions between CSIRO scientists and officials of those departments. That is all I know of at this stage. If you are asking if there is a formal briefing on a weekly or monthly basis, the answer, to the best of my knowledge, is no. Do we have good links into there? I believe the answer is yes. Could they be better? The answer is 'of course'. With unlimited time and resources we could all do these things much better.

CHAIRMAN—Are you asking for more money!

Dr King—No, I was not!

Ms GRIERSON—A question that is often raised in the public is about the current screening equipment and whether it has any risk to humans in terms of radiation or whatever. Can you comment on that?

Dr Floyd—I am aware that the levels of radiation exposure for some of the technologies that are being looked at are far less than the radiation you are exposed to when you are in your kitchen. It is useful to keep these things in context and have some view of the relativity.

Ms GRIERSON—I think that is important. People who once used to put their feet in X-ray machines as kids et cetera have learned too late that we do need to make sure that prolonged use of these devices does not have any risk. That is important to the public.

Dr Giugni—To follow on, I think there is a greater degree of exposure associated with the flight than with the scanning.

Dr King—If I can venture one other comment here, one of the advantages of one of the technologies that we mentioned in our submission—the passive millimetre-wave imaging—is that it senses, essentially, radiation we all give off, as opposed to subjecting people to radiation. So that is an advantage in perception even if it is not an advantage in reality.

Ms GRIERSON—What stage is that technology at?

Dr King—It is being prototyped in laboratories now. It is very high tech, and I would not expect it to be out in the community for some years.

Ms GRIERSON—Do you think it would be cost effective, if it ever became operational? Would it be similar in cost, or would it be more expensive?

Dr King—The intention is to get it down so that it is cost effective, certainly.

Ms GRIERSON—You talked in your submission about airspace modelling. I suppose we expect too much of technology at times, and we think you know where all our planes are all the time. Obviously that is not the case. Can you explain a bit more about airspace modelling and about what the risks are of gaps in information? What can be done about that?

Dr Fulton—The real issue is that in a safe and secure environment you need physical knowledge of the entities that are flying around, the aircraft. Even with knowledge of those aircraft, September 11 type accidents could happen, because you also need to know the intent of the pilots. The first step is knowing where aircraft are, for a number of different reasons—defence, customs, physical proximity and so on. At the moment, we do not have a high knowledge of all aircraft movements. A second point is that there is progress beyond what is happening here. There is international progress in understanding how to sort out aircraft flows, knowledge and so on. It has been a very complex mathematical problem, but in the last decade significant advances have been made. Also, there have been significant advances in the technology of communicating between aircraft. To bring it back into the public arena, the mobile phone is an example of how technology has changed over the past decade.

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

Ms GRIERSON—So you could program it in if you saw any deviation?

Dr Fulton—You could then start to talk about more intelligent interpretation of what is going on. But you need to know where that aircraft is in the first place.

Ms GRIERSON—How reliant are we on satellite technology and access for that sort of information?

Dr Fulton—In the civil arena, there is communication by satellite, which makes it easier to communicate between aircraft. There is also the terrestrial based communication system, which

has been in place for many years in aviation. If you are talking about surveillance, like military surveillance, I am not really qualified to say what that can detect.

Ms GRIERSON—There was a question from the chairman earlier about the human aspects. We see all sorts of technology being subverted in its application by human behaviour. Being from Newcastle in New South Wales, I have looked at the way train drivers interfere with the application of fairly important pieces of equipment. I would think, if we are trying to develop a security culture, that human behaviour and ways to impact on it would be extremely important. I would also have thought that CSIRO would have experts in that field. There must be ongoing research, but is any specific research being undertaken that targets human behaviour in security environments?

Dr King—To the best of my knowledge, the answer is: not in CSIRO. We tend to be working on the physical and technological aspects and increasingly recognising, as you have done, that they are only half the picture. But in those matters, rather than employ that expertise ourselves, we tend to rely on working with partner organisations.

Ms GRIERSON—We do tend to overlook that essential element—the human factor and its power. At the moment, for security and safety reasons, is CSIRO involved in aircraft design? I know you have mentioned some acoustic wave devices that look at spaces and vacuums or empty areas, but is CSIRO aware of or involved in any other work associated with aircraft design to perhaps make aircraft less dangerous?

Dr King—The acoustic testing device is the only one that I know of. It is aimed at new aircraft construction using composite materials with laminates in between. If damage is done to aircraft constructed of these materials, it is very difficult to see any sign of it from inspecting the outside of the aircraft even though it is compromised on the inside. This technique is about determining damage in the new types of materials, and it is mostly to do with that aspect of it rather than with the design of aircraft from an enhanced safety aspect.

Ms GRIERSON—Does it ever occur to CSIRO that this field of aviation security perhaps has some great economic potential as well and that perhaps we could target our research to get that cash flow up a bit?

Dr King—It is interesting that you mention that, because it is certainly true. The federal government has identified having a secure Australia as one of its national priorities. Certainly CSIRO is spending roughly $100 million a year on that aspect. But that is very broad. It goes all the way from protecting us against invasive pests and diseases et cetera as much as protecting us against terrorism, and we are certainly spending far less on the counter-terrorism aspects. But we are working with the new PM&C unit, the science and technology unit, trying to identify where there are gaps not just in CSIRO but in Australia. We are working with our other agencies, such as DSTO and ANSTO et cetera, so that we can plan out some research that makes sense in this area to fill in some of those gaps. But we are not going to see the fruits of that research, by its very nature, in a short time scale. September 11 is two years ago now and we are identifying work that exists in other fields that has application in this area now, and we can do that. But I think you are asking: what are we going to do that is new that will give us benefits in five years time? We are certainly working on that.

Ms GRIERSON—What about this low-pressure plasma device? What on earth is that and what does it do?

Dr Floyd—This is a device that can be used in an airconditioning system, in a building or in an aircraft, that can destroy micro-organisms. In the context that you are in a confined space for a number of hours in an aircraft, there is obviously some vulnerability around this area. If you had some system that could detect and then be activated to destroy micro-organisms, it would be very helpful.

Ms GRIERSON—Would that have health risks too? I am sure that what was being detected would have a higher health risk, but would this system have health risks too?

Dr Floyd—As far as I am aware, there would not be any health risk to passengers because you would have this with the air treatment system of the plane. The work that is going on at the moment is focusing on buildings and building airconditioning. It is a matter then of taking technology that is being developed in that domain and looking at how you could use it within a smaller domain, such as an aircraft.

Mr JOHN COBB—You have provided us with very interesting information. You talk about interference with operational systems in flight, virus toxins et cetera. Even though you have the cabin shut off, is it a possibility that somebody could introduce toxins or whatever in the system in an aircraft and then take control of the aircraft without actually being in the cabin?

Dr King—Off the top of my head—and I am not an expert—that would seem to be difficult to me.

Mr JOHN COBB—You talk about interference with operational systems in flight. Obviously that might be just to upset them, but would it be possible to take control of the aircraft computer without actually being in the cockpit? It just opens up a rather disturbing—

Dr Floyd—I do not think we are in a position to be able to comment on that, as much as my sci-fi thinking would go into all sorts of possibilities. But that illustrates the need to have the dialogue from a range of perspectives so that people who are not in the aviation area but have knowledge of certain technologies get together with those who intimately know the details of the aviation industry and throw around those sorts of ideas.

Mr JOHN COBB—I feel a little better. You talk about a lot of different technology, such as high-speed and passive imaging, acoustic waves et cetera. I take it that a lot of this is still in the maturing process—things that you are working on?

Dr King—It is at various stages. Some of those are no more than laboratory prototypes that may be too big or costly before they go further. Some of them are at the stage of undergoing trials in the community at the moment, and for others those trials have been done and they are in the process of being commercialised. There is a whole spectrum of stages of development there.

Mr JOHN COBB—So we still have a fair way to go to get some of this stuff right? I am not being critical; I am asking a question.

Dr King—That is correct, in the sense that they are technologies that were generally developed for some other purpose and we are now looking to see how they can be applied in this particular area post September 11, and that takes some time.

Mr JOHN COBB—Would it be fair to say that we are probably going to end up with a combination of the lot of them? Reading through your information here, it seems that some will do one job but not the lot.

Dr King—And undoubtedly there will be technologies from many other technology suppliers. Australia does approximately two per cent of the world's research. Even if we are world class and do something special in some of these technologies, we need to be realistic and expect that most of them will come from overseas, just because there is the resource issue.

Mr JOHN COBB—Reading that, I would assume that what we are using now, while it may be world's best as of now, is not getting it all and, short of a body search, you are not going to detect all the possibilities.

Dr King—That is correct. Just as in medical research people use X-rays, CAT scans and MRI and they overlay the three and get much more information by doing that, you can see with this issue that different techniques will give different bits of information and together you form a much bigger picture.

CHAIRMAN—Thank you very much once again for your submission and for coming and talking to us today. If we have further questions, you will not mind if we put them to you in writing?

Dr King—Not at all.

[12.09 p.m.]

BATMAN, Ms Gail Jennifer, National Director, Border Intelligence and Passengers, Australian Customs Service

CHAIRMAN—Thank you for coming back today. I must admit to not being overtly happy to have to ask you to come back, because you appeared before the committee yesterday. On my way to Parliament House this morning, I was listening to ABC radio and I discovered that last week—on Wednesday, the 22nd—two Customs computers were stolen from a Sydney airport area. I would like to know why you did not tell us about that yesterday, since we were inquiring into aviation security.

Ms Batman—I can certainly understand that you might be alarmed after having read the articles and the news today. Although it is a breach, and certainly a very serious security breach that we are taking seriously, it is not a national security breach—the Attorney-General confirmed that this morning—and it is not an aviation security breach. The theft occurred in a Customs office building that was on the perimeter of the airport, but the investigations conducted since that time have shown that there is absolutely no evidence that those servers contained the thousands of confidential files that the newspapers claim. The servers did not contain any personal, business related or security information at all, and they were not servers that were used to communicate with law enforcement or security agencies. The other reason that I felt it was not appropriate to mention this yesterday is that there is an ongoing investigation into this. It is a criminal matter. The AFP are investigating it and have not yet concluded that investigation, and we certainly do not want to compromise that. The people who stole these servers are certainly ones whom we want to see caught and prosecuted.

CHAIRMAN—We have a very open society, and we highly value freedom of the press. Surely you must have known that the press was going to get a hold of this story. Knowing that the press was going to get hold of this story, I fail to understand how you could come before the Public Accounts and Audit Committee—one of the most respected parliamentary committees in this parliament, which has been in operation for 90 years—and not tell us about this security breach. It is beyond my comprehension.

Ms Batman—We did expect that immediately after the incident the story would be in the press. When it did not appear, we all assumed that it would not. If it had not been for this leak—I do not think this is an appropriate matter to be canvassed in public in the middle of an investigation. We really need to have the investigation brought to bear on this. As I say, it is a very serious matter. I do not want to downplay it in any way but, while it is a security breach, it is not an aviation security breach.

CHAIRMAN—You are well aware that this committee has not yet completed an inquiry into information technology security in the Commonwealth environment, and one of the things I can guarantee you that we never considered was the theft of a mainframe. I have just instructed our inquiry secretary to reopen the hearings and the inquiry. Perhaps I am wrong, but it seems to me that, if someone can walk into a government secure environment and walk out with mainframes, then I do not know what guarantee we have of information technology security.

Ms Batman—I think one of the themes you will find through this inquiry is that, no matter what technology and no matter what systems you have in place, the real key to any security comes down to people. The human factor is one that is very hard to take account of. Any breach of security is an opportunity to learn more, and we are investigating this and learning all of the lessons that we can. We have taken a number of steps already to tighten our security and our access control for visitors coming onto Customs premises and certainly the ones in a tradesman or technician capacity. We are learning all the lessons that we can. I do not wish to belittle this in any way; this is a serious breach. It should not have happened. We are doing all that we can to learn from it, but ultimately humans are human and errors do occur.

CHAIRMAN—If the information stored on those two mainframes is of no commercial value, no security value and does not include passwords of Customs personnel or other personnel interacting with the Customs system, why on earth did they steal them?

Ms Batman—It is a good question. We hope the answer will come to light in the investigation.

CHAIRMAN—They have just stolen a couple of innocuous computers that are of no value to anyone?

Ms Batman—That is really part of the investigation, and it is beyond my technical knowledge as well. The technical aspects have been investigated for a week now. There is no evidence, as I said, that they contained any personal information, any business related information or any security information—

CHAIRMAN—No code?

Ms Batman—and they were not a communication device.

CHAIRMAN—There was no code, no encryption systems?

Ms Batman—None of the above. My technical knowledge is extremely limited, but we have experts from the AFP and from security agencies working on the system at the moment—they have been working on it since that time—and all I can say again is that, to this point, there is no evidence that any of that information was on those servers.

CHAIRMAN—Okay. I can say this to you honestly: this committee has no desire whatsoever to compromise any investigations or any possible subsequent prosecutions. We do not act like that; we are responsible. But we do want answers as to how on earth we could have such a serious information technology security breach—and in an airport area.

Mr JOHN COBB—Ms Batman, you say this was not an international breach because the computers did not hold codes or personnel files et cetera for Immigration. I am aware that you do hold the mainframe on behalf of Immigration—or you hold information for them on the mainframe.

Ms Batman—We have a live connection to Immigration. Maybe I could just correct you as well: they were not mainframes, they were servers. My technical knowledge is just about exhausted at this point, but I do not think they were mainframe computers.

Mr JOHN COBB—Be that as it may, would it have been any different or any harder for whoever the perpetrators might be to have actually got that sort of information? They obviously did not have much trouble getting the computers. Would it have been any harder for them to get into a situation where they could have come out with personnel files, codes and passwords than what they have already done?

Ms Batman—All I can say is that over the last year we have tightened our security procedures. We have been over them several times and we are going to do that again. Every time you get a breach you learn more. We will learn more.

Mr JOHN COBB—That was not what I asked. I meant: did the same building house other, more sensitive or more international files and computers?

Ms Batman—I am not aware of what else is in that building.

Mr JOHN COBB—It is a little disturbing to think that they could have taken all those codes and all Immigration's personnel information so easily.

Ms Batman—I am just not aware what else is in that building. The equipment is not Customs owned; it is owned by our IT supplier EDS. It is their equipment that provides our IT service in our premises. Certainly I am acknowledging that this was a serious breach.

Mr JOHN COBB—I would like you to take that question on notice and get back to us as to whether or not the information could have been as easily accessed.

Ms Batman—Certainly.

Ms GRIERSON—Firstly, I find it very difficult to accept that a server, then plugged into a computer with ordinary software that we all have access to, would not become a communication device and would not then give access to anything that is stored on that server. If the information stored on that server is not about passenger movements, Customs processes and Customs personnel, then what else is on there? It would seem to me that that is your main business and would certainly be on any computer system that you use. I also was alarmed to hear DIMIA say that they have that interface with your mainframe—the information that DIMIA hold is quite extensive and certainly there are a lot of human records. To us it is very alarming news. That you did not tell us also prompts us to ask: what did you do when that breach happened? Who did you tell? What processes went in place straightaway in terms of people's access to information that possibly would be on that computer?

Ms Batman—As soon as it came to light we informed the local state police at Mascot. We have informed the Australian Federal Police, ASIO and DSD. As a precaution we took immediate steps for all our staff to change their passwords.

Ms GRIERSON—When you say 'straightaway', what was the time limit?

Ms Batman—I would have to take on notice details of the timing. I could give you some details of that, but it was certainly at around the time of the incident. It did take us some time to try and ascertain what might have been on those servers at the first instance, what we needed to do and what steps we needed to take. As I say, we had all of the staff change their passwords on a staged arrangement, which took some time because, as you can appreciate, people are on shift arrangements. As people came into work we had everybody change their passwords as a precaution. We have asked staff to report anything that they feel might give any indication that something is wrong with the way they use the system. We have had the AFP and DSD examining the computer systems so that we can try and work through what might have been there. That was done in conjunction with EDS—as I say, it was part of their equipment.

Ms GRIERSON—We also have some concern that this building was specifically targeted and perhaps those file servers were specifically targeted with a malicious intent and for a specific purpose. It does not seem that they were just after computer equipment; it seems that they were after specific Customs related equipment. That would perhaps suggest that there could be some internal security risks that need to be responded to. Have you done anything to screen your internal processes and your personnel?

Ms Batman—Yes. We took immediate steps, certainly, to ask all our regional security advisers to review access controls, particularly for visitors on all of Customs' sites. We have gone back and asked for them all to provide details of what happens in all circumstances. We are talking to EDS and their subcontractors about arrangements that can tighten controls in terms of their visiting technicians. We do security clear all of our staff and all of the EDS personnel who work on our account. Anybody else that has regular contact has to have a security clearance, including all of the contractors. There are the one-off visitors, and we have procedures for escorting them. We have reviewed all of that and we will continue to do that. I can assure you that we are taking a very thorough approach to that.

Ms GRIERSON—As this was a building at Sydney airport, what communications and procedures have Sydney airport changed in their approach to security as a result of the breach?

Ms Batman—The building is on the perimeter of the airport. I am not sure if you know Sydney airport, but it is the blue building—a squat blue building over to the side, near where the cargo and mail planes are, near the mail-handling unit. Although it is on the fence line of the airport, it is a separate office building.

Ms GRIERSON—Do you know how those people gained access to that building?

Ms Batman—I think those sorts of details are really a matter for the investigation.

Ms GRIERSON—You have presented today, but is there someone at Customs who is in charge of security?

Ms Batman—I hate to say this, but physical security is my responsibility—not the IT part but certainly the physical security is part of my responsibility.

Ms GRIERSON—I was surprised by DIMIA's reaction. They were unaware of that breach, yet their mainframe interfaces with yours and they would have been instantly alarmed. Why were they not informed?

Ms Batman—It was because we had this advice that said there was no connection. It was not that information, it was not that computer system and none of that information was there.

Ms GRIERSON—If it is appropriate for me to ask you this and for you to say it in public, could you tell me what was on that equipment?

Ms Batman—There are two things: one, I do not know and, two, I do not think it is appropriate to say at this stage.

Ms GRIERSON—Okay. I think, Mr Chairman, we will probably want a little bit more information at some stage about the processes followed and the outcomes of the investigation.

CHAIRMAN—I think we want answers to a whole heap of questions, Ms Batman. I think we will let it go for today. The committee will convene next week and decide how it wants to pursue this issue. Could you answer one question for me, though? I am a little bit confused about where this building is; is it inside or outside the perimeter fence of the airport?

Ms Batman—It is outside the perimeter fence but on the perimeter fence, if you like, and there is a gate through, from memory—but it is outside.

CHAIRMAN—Are you telling me there is a gate into the building from within the airport?

Ms Batman—Yes, but it is a secure gate. It is not inside the perimeter fence; it is adjacent to the perimeter fence, with separate access. You do not need to be inside the airport perimeter fence to go in and out of this building.

CHAIRMAN—It would seem to me that it was not too secure, or we would not be missing two servers. Thank you for coming today. The committee will consider how we want to progress this issue. Any information you receive that you can give to us which does not compromise the investigation or any subsequent prosecution we would appreciate receiving in writing as soon as possible—

Ms Batman—Certainly, I will give you that.

CHAIRMAN—or else come back and talk to us again—either or both. Thank you very much.

Proceedings suspended from 12.28 p.m. to 2.13 p.m.

LEWIS, Dr Edward James Essington, Convenor, Australian Identity Security Alliance

CHAIRMAN—We will resume this public hearing. I advise witnesses that the hearings today are legal proceedings of the parliament and warrant the same respect as proceedings of the House itself. The giving of false or misleading evidence is a serious matter and may be regarded as a contempt of parliament. The evidence given today will be recorded by Hansard and will attract parliamentary privilege. I refer any members of the press who are present to a committee statement about the broadcasting of proceedings. In particular, I draw the media's attention to the need to report fairly and accurately the proceedings of the committee. Copies of the committee statement are available from secretariat staff. Dr Lewis, we have received your submission. We thank you. I am not sure I understand it, but anyhow thank you. Do you have a brief opening statement before we ask you questions?

Dr Lewis—We would like to make an opening statement for three reasons. Firstly, we would like to clarify whatever it is that you do not understand. Secondly, things have been changing rapidly as far as the alliance is concerned, and the circumstances that led to the building of the alliance have been changing rapidly; we need to bring things up to date in that regard. Thirdly, we have been attending for the last couple of days and hearing what other people have to say, and that has led to the need to perhaps make some further clarifications or responses.

CHAIRMAN—Will you keep it very brief? Otherwise, we will run out of time and then we will not get to ask you questions and that means we will have wasted the hearing.

Dr Lewis—I will move on quickly to the objective of the alliance, which is in the material that Ken Hyams, our secretary, has sent to you. The membership has changed in that we have added three Australian organisations: Phoenix, which is a risk management consultancy; VeCommerce, which is a speech recognition and speech biometrics consultancy; and Interface Pacific, which does a lot of work on face based systems. They are now part of the alliance as well as the firms and organisations that are already on the list that you have, including CSIRO, Damovo and the like.

We did want to make some points based on our experience in this area of identity security, which goes back a number of years. Some of the members of the alliance have been talking to people like Customs and the Attorney-General's Department about this issue since 1994. They have a patent in this area which was prior dated back into 1995, which is an issue that should be taken into account when we are looking at things like SmartGate and the rest of it. Others have been working in areas of identity fraud—be it in voter fraud or data assurance—for a number of years. In fact, I was doing some policy work for Visa in Singapore on 10 September 2001, so our activity certainly predates any trigger events that might be related back to September 11 of that year.

Our reason for being has primarily come about through a sense of frustration to see what approaches are currently under way in identity security not only for things like aviation security but, of course, throughout the whole area of identity fraud and identity theft and what that means to Australia in terms of economic damage as well as the obvious terrorist damages. Basically, our view is that the approaches that are undertaken are limited both in scope and in depth. There

are certainly lots of attempts to build what we would call a security chain. If you look into identity security starting well before the enrolment of people and going through to what happens when you detect and how you react to people who have been found to be causing mischief, at the moment we have different organisations and agencies doing little bits in little places. Although there is meant to be a layering approach to security in our field, there are too many gaps and broken links in the chain, and we as an alliance are trying hard to do something about closing those gaps. An example would be the sorts of things that have been spoken about today, such as the dependency upon PKI. Although my background is not in encryption, some of my colleagues are world authorities on encryption and our suggestion would certainly be to double-check PKI as a secure system, especially when it depends upon keys stored on mobile servers or mobile laptops.

There are issues of protection of identity that people are not looking at in terms of side channel attacks on smartcards—that is, the ability to attack a card and to break its code through physical means rather than through electronic means—and what you could call sledgehammer attacks like the one at Customs last week, where somebody breaks in and steals things. They include the several hundred laptops which are lost out of government agencies each year. The whole issue of—

CHAIRMAN—Thousands.

Dr Lewis—Yes, thousands.

CHAIRMAN—Not hundreds.

Dr Lewis—We were trying to be conservative and not to engender too much fear in the process. There are issues, of course, of identity fraud involving the administrators, trusted insiders, that need to be looked at as well—for example, people walking in using false signatures to give themselves access to a computer system for two hours before they actually steal it. That is an example of the depth that you need. It is not just a matter of protecting a computer system or protecting one single point of entry; it is a matter of protecting the whole ring of things around these security gates or computer systems.

CHAIRMAN—Did you really give that serious consideration before today?

Dr Lewis—Always.

CHAIRMAN—So somebody might steal the mainframe?

Dr Lewis—Yes, it has happened a number of times.

CHAIRMAN—Somebody might steal the database?

Dr Lewis—Yes, sure. It is part of the policies we have established for some of the other agencies we have worked for. A number of people depend upon a pin code system on a normal interior door. That is the security for their computer room. As I say, the loss of servers and machines has occurred in many organisations around the world in a whole variety of ways.

CHAIRMAN—So they have actually stolen the hardware?

Dr Lewis—Yes, sure. If you want to get hold of somebody's data then all you need to do is get hold of one password to make life difficult for the whole system. If you just want the data, if you want to see who is a person of interest, then you steal the data. You do not have to worry about the fact that you have left behind a hanging door. If you have your hand on the data then you have achieved your objective. It is only the people who want to sneak in and not leave a trace behind that people worry about. But there are people who will break through; they will come through the ceiling or break down the door. That is what T4 security is meant to prevent.

The other aspect is that people themselves need to be protected. You need to protect people against people who are misusing identity in one form or another, either through theft or through fraudulent representation. Another issue is that there are now movements towards biometrics, but again they are limited in their scope. They are using single biometrics instead of multiple biometrics, as is recommended. They are using a single data source for the biometric check instead of a three-way source—that is, a first enrolled, last enrolled system—

CHAIRMAN—What does that mean?

Dr Lewis—I will use an example which comes from a patent held by one of our alliance members, a firm called P7. They have established a process where, basically, when you first enrol, the biometric information is stored on a database under that organisation's control, but when you are last seen by the system—the last time you flew out of the country or the last time you borrowed money from a bank or whatever—your biometric is re-enrolled and that is stored on that database under that organisation's control. We are not talking about biographical information; we are just talking about biometric information which is linked to a token: a card, a passport or a document of some sort. When you come through a check-in process now—if you come through a gate or come into an airport under the better systems that are around—it compares both databases, not just the one. In order to provide better security for the total system, you need to have several sources so that if somebody has suborned one source then they need also to have suborned another. Otherwise, the match will not be made. That is what we call three-way matching.

CHAIRMAN—Does that have privacy implications?

Dr Lewis—Certainly, and one of the driving objectives behind the alliance is to provide easy access to authorised people whilst maintaining a concern for privacy. That is why I mentioned making sure that biographical information—that is, information such as name and address—is not necessarily held with biometric information. You can be cleared because you are the person holding a token and the authority to enter is based around the token; you do not necessarily have to keep names and addresses for who received the token or who is using the token at any one time. You can separate those things out. The system design has to do that separation.

There are gaps, and I think people have been looking in the wrong place. That certainly came out this morning. A lot of emphasis has been on technology and not enough has been on people; that is why it is reassuring to hear the commentary from the members of the committee about the importance of people. That is our view, and that is why I was tempted to stand up behind CSIRO

this morning and wave and say, 'That is what we do.' We are concerned about the people in the process, because that is where the weak points are.

It was interesting that recently when the Academy of Science had what they called the young high-flyers workshop on securing Australia—to which I for some unknown reason was invited; I do not think I am either young or particularly high-flying—they had a number of scientists looking at the issue of how science can help in safeguarding Australia, and the point for all of them, including the hard scientists, was that it was to do with people, not the science of pieces of equipment. As a psychologist with a PhD from Newcastle, I would obviously share that bias. We have got to be involved in acquiring a better understanding of people who might provide the attack and a better understanding of the people who provide the defence in these systems. More importantly, we have got to develop people-proof procedures so that we understand that you cannot depend on training and you cannot depend on people knowing or understanding policies; you have got to look at procedures that take into account the frailty of humans and build in fail-safes.

The other aspect is coordination of research—or the non-coordination of research in this area. You have heard from CSIRO, and they have mentioned DSTO but, of course, I come from the University of New South Wales at the Australian Defence Force Academy, so my interest has always been the science that is carried out in the university sector, of which there is an enormous amount. The day before yesterday we had a meeting at the academy to identify who was involved in research to do with security, and there are just a dozen people in a very small faculty; around Australia, there are probably thousands. At the moment, we have a survey into science and security, but there is no direction at this stage.

We are working with Standards Australia to develop a process standard that helps us cover the whole gamut of links in the chain. I am on a biometric standards working group that is involved in this sort of thing. It is chaired by Passports Australia, and we are now raising officially with Standards Australia the need to build this end-to-end process standard to cover identity related security, where the various biometric standards fit into one spot or another. We are also beginning to work on a series of workshops for a whole-of-government approach, and we have been talking with DOTARS about that. We are trying to contribute to the research networks that are being established by the Australian Research Council.

Finally, we are trying to develop a series of prototypes to get over the issues that have been spoken about so that we can have security at regional airports that is not expensive. There is no need for gates for the checking of people going on aircraft; members of the alliance have other technology which can check if a person is authorised to be on the airfield. You do not need to see somebody's face to see if they are authorised. Through RFID and other technologies—

CHAIRMAN—Hang on; we do not know what RFID is.

Dr Lewis—They are radio frequency identification devices. They are the little chips you can these days add to banknotes and use to replace barcodes.

CHAIRMAN—Do you implant it in your skin?

Dr Lewis—You wear it like a flight pass.

CHAIRMAN—But why couldn't somebody else take it?

Dr Lewis—Then you link it to your biometrics. This is where the interaction between these systems comes into place. You can store the biometric information—

CHAIRMAN—What is the biometric information that tells you that that is now not valid?

Dr Lewis—You have a variety of biometrics—

CHAIRMAN—Such as?

Dr Lewis—Thermal patterns of the face rather than the visual patterns of the face; speech, of course; gait; and even, crudely, height. But you would not have one of them; you would have several of them. So depending on how you set up your enrolment process—

CHAIRMAN—That sounds pretty expensive.

Dr Lewis—That is right. But the expense is in the enrolment process; it is not in the device. The device you are talking about is worth cents. Wireless transmitters or things that you might have in airports or on airfields can obviously be expensive but, compared to a whole array of gates, they are cheaper. Certainly compared to the staffing that is required for face-to-face identification, they are cheaper. As soon as humans get involved in the process, there is the labour cost—that is the expensive part. That includes, in this case, the enrolments. So how do you capture the biometric simply and easily? It is one of the things we are trying to develop in the prototype system we are putting together.

CHAIRMAN—I could take Dr Carter's pass to Parliament House and that will get me into the car park, but then I have to come past the scanner to get into either the House of Representatives or the Senate. I guess you could even come in the main entrance or the ministerial entrance. Once you scan the pass, your photograph, which is stored on a computer file, comes up on the computer screen. Even though I have got his pass, I do not think I would get away with getting into Parliament House, because I do not look much like John Carter.

Dr Lewis—Do you have a good biometric system in place now?

CHAIRMAN—We must; that is it.

Dr Lewis—It is not a biometric system if it is not compared against some physical characteristic. You have a biometric system in that there is a guard that would look at it. A guard is a biometric system in the sense that they will compare a face against what is on the photograph—assuming they do actually look at the photograph. That is called a one-factor system. If you have just got a card that you can swipe against the door, there is no guarantee that you are the authorised user of that card. As a pickpocket I could have stolen it from you coming through.

CHAIRMAN—I understand that; we know all of that.

Mr JOHN COBB—Dr Lewis, I gather that most of the stuff you are talking about is still being developed.

Dr Lewis—Not all of it. Some of it is available now and some of it will be available shortly, depending upon action that is happening here and overseas.

Mr JOHN COBB—Let me ask you a general question then: given the technology available, do you believe the systems we have in place at our airports are as good as we can do?

Dr Lewis—No.

Mr JOHN COBB—Why are they deficient?

Dr Lewis—They are deficient because at the moment they are isolated systems; they are not necessarily integrated into a total system that has secured all points in the linkage.

Mr JOHN COBB—Are they not integrated for one to work with another or are they not integrated with the relevant department, whether it be Townsville to there, Darwin to there or Sydney to there?

Dr Lewis—All of those, horizontally and vertically, if you want to set it up as a framework of process. There are various steps you need inside a security system and there are various layers of things that are necessary to support the system. They are technology, human skills, work practices and the policy of the agency to make sure people are actually using the technology correctly. If you want to see it as that table, there are gaps in various parts of either process or layer at the moment. That is not a criticism.

Mr JOHN COBB—Is it being addressed?

Dr Lewis—It is being addressed in part. We understand there are whole-of-government studies that are under way trying to look at some aspects of it. As clients there is not much being done from the suppliers of these sorts of systems to come up with an integrated system, and that is why—

Mr JOHN COBB—By that, do you mean the CSIRO?

Dr Lewis—No, I mean private sector firms that sell this sort of system.

Mr JOHN COBB—Be it IT or be it actual technology?

Dr Lewis—All of it—not just the technology, but also the training of the staff and the development of the policies within an agency and so on. There are some people who do a variety of integrated things and you have got submissions from some of those people already, but we think there needs to be a coordinated process from both the supplier and the client.

Mr JOHN COBB—And who should coordinate that? Should it be DOTARS?

Dr Lewis—Who benefits? Cui bono, to use the—

Mr JOHN COBB—We all do.

Dr Lewis—Exactly, and this is one of the reasons why we are a bit surprised about the attitudes of airport authorities and some of the airlines.

Mr JOHN COBB—You are going to have to be a bit clearer about who you think should be coordinating it.

Dr Lewis—At the moment there are national implications, both in security and in economic terms, so the agency that is responsible for the national security of aviation should coordinate it. In that case, it is DOTARS. If you are looking at access control into computer systems more widely, because that is part of the chain, let us take the MAL lesson, the system that DIMIA runs. Who is the agency that is responsible for the security of all the government computer systems that connect to each other? Who is the agency responsible for coordinating long-term research for national or economic benefits? We do not know the answer to that. One of the difficulties that we have had is actually finding out—and obviously you have as well—who should coordinate it, because everyone is going off in different directions.

Mr JOHN COBB—So you are not making any suggestions?

Dr Lewis—We would like to see the National Security Division in PM&C taking a role. They have the science and technology unit to start some of the coordination and they have the brief to do some of the coordination across the agencies.

Mr JOHN COBB—That is the division of DOTARS that you are talking about?

Dr Lewis—No, it is in Prime Minister and Cabinet.

Mr JOHN COBB—Sorry, yes. DOTARS have their own security division as well.

Dr Lewis—Sure, but Prime Minister and Cabinet are in a position to coordinate DOTARS with DIMIA, with ACS and so on.

Mr JOHN COBB—You mean the senior executive one?

Dr Lewis—Yes, and there are some working groups in that area. One important part of it is to have agencies asking for an integrated approach; it is another thing to have people able to provide the integrated approach. Coordination is needed there.

Mr JOHN COBB—Have you approached Prime Minister and Cabinet and made any suggestions to them on this?

Dr Lewis—We have approached some of the agencies. We have only recently become aware of some of the other coordinating activities under way in Prime Minister and Cabinet and in the Attorney-General's Department. We have not yet approached them because we were not aware that they were there.

CHAIRMAN—This can get awfully expensive, can't it?

Dr Lewis—It can. It does not have to be, though.

CHAIRMAN—Gatekeeper is a relatively secure certification authority working with encryption codes in PKI in order to try and keep the Commonwealth IT in a secure environment where the Commonwealth is dealing with outside agencies, but it is also terribly expensive and terribly slow and there are modern technologies that might replace it.

Dr Lewis—Yes, exactly. That is what the alliance is trying to develop.

CHAIRMAN—I understand from a discussion I had with a gentleman recently in my office that there is new technology which could produce—or does produce, wherever it has been used—a password code that regenerates itself every few seconds. The receiving code also regenerates itself every few seconds and the possibility of even one of the world's largest supercomputers breaking into that system is so ultraremote as to be laughable. Are you familiar with such systems?

Dr Lewis—Yes. RSA cards and so on have been around for a while, which are in that sort of family of systems. Until quantum computing gets going—

CHAIRMAN—But this is both sides of it: both the source and the receiver. The receiver is identified and guarantees it is the receiver, the source guarantees it is the source and the transmission is not, theoretically, hackable.

Dr Lewis—That is right. There are several other modern developments. Quantum computing key management systems—the sort of work that is coming out of ANU—are certainly making major differences in the sorts of things that you can do for encryption security in transit. But, at the same time, quantum computing is putting up major challenges to all of that as well. But that is not enough.

CHAIRMAN—The point I am trying to make is that we can get too expensive and we can become too time consuming.

Dr Lewis—Yes.

CHAIRMAN—There are a lot of organisations that would like to participate in Gatekeeper, for instance, but my advice would be not to because it takes so long to become certified and it is so expensive.

Dr Lewis—My advice would be not to take part in it either. There are other reasons why I would give that advice, but cost and labour are certainly part of it.

CHAIRMAN—You did not appear before the hearings on that inquiry.

Dr Lewis—No, but I did read them.

CHAIRMAN—I do not know whether or not we can transfer information across—I doubt it.

Dr Lewis—But that is the whole idea: there are arrangements you can do with biometrics based encryption, for example. There are arrangements to protect the tokens or to protect the devices that transmit the message. There are devices elsewhere down the chain so that somebody coming in with a false signature does not take the equipment away. That is what I mean by the different layers of security you have to have in these sorts of systems. It is not enough to depend upon one device talking to another device. Can you trust the person at either end of that chain? If I wanted to steal secrets, I would use a social engineering attack—and I know you have heard about those. In other words, I would come in and try to pretend that I was somebody else and convince somebody inside the system to give me access. Kevin Mitnick's book gives a good example of how many organisations will freely give away passwords because they think you are an insider.

CHAIRMAN—We can talk about the gaps and we can talk about the problems in aviation security to such degree that we so frighten the public that the public does not want to travel anymore; therefore, we might as well not have talked about it because there are no aircraft in the skies.

Dr Lewis—Yes, we paint that scenario as well. The safer system is one that nobody actually uses. It is a very *Yes Minister* approach, of course. That is why we are trying to come up with systems that are secure, that have good privacy and that are cheap enough to institute compared to the risks you are facing.

Mr JOHN COBB—You talk about having effective security while maintaining all the freedoms. Seriously, is it possible to have the ultimate security and not impose upon people's freedom? Personally, I think people will put up with a little bit of that to feel safe, but I would think it is something of a contradiction in some circumstances.

Dr Lewis—It is certainly a balance. It is really a balance of two risks and so you have to take fairly traditional risk management approaches: the consequence of a security breach against the consequence of a privacy breach. There are all sorts of issues underneath those two simple comparisons, but that is basically what you have to look at application by application. Some people do not mind giving up their privacy if it means that they can fly safely; other people will fight if it means that their health records are released.

Mr JOHN COBB—The way that you have written it here in your submission indicates that you seem to think one is contingent upon the other, which I do not really think it is.

Dr Lewis—I agree with you: no, it is not.

CHAIRMAN—Dr Lewis, thank you very much for your submission and for coming to talk to us today. Technologically, you are so far above us poor mortal souls that I am not sure we understand everything you have been talking about, but we appreciate your contribution and I am sure that you and your organisation will continue to advise the bureaucracy on more modern and better ways to go about securing both our skies and our IT systems.

Dr Lewis—Thank you, Mr Chairman. I have one final point. I live a kilometre that way and I work a kilometre that way, so I am here to serve.

CHAIRMAN—If we have more questions, I am sure you will not mind if we direct them to you during the course of the inquiry.

Dr Lewis—I would be delighted.

CHAIRMAN—Thank you very much.

[2.45 p.m.]

WILLIAMS, Mr Clive, Strategic and Defence Studies Centre, Australian National University

CHAIRMAN—Welcome. You did not give us a submission; you came and talked to us off the record.

Mr C. Williams—I have a submission I can give you today if that is all right.

CHAIRMAN—Fine. Would you like to make a very brief opening statement?

Mr C. Williams—I was just going to read through my submission. Is that what you would like me to do?

CHAIRMAN—How long will that take?

Mr C. Williams—Probably about 20 minutes.

CHAIRMAN—No, I would prefer not, because there are many questions that we would like to ask you.

Mr JOHN COBB—We would like it, though.

CHAIRMAN—Yes, we would like to receive it as evidence. If you could summarise it in three or four minutes, that would be helpful.

Mr C. Williams—I will paraphrase it. I will summarise as I go along.

CHAIRMAN—Otherwise we will not get to ask you questions.

Mr C. Williams—Basically, what I have come up with is suggestions in a number of areas. These relate to intelligence, aircraft, flying staff, airports and legislation. Firstly, in the area of intelligence, I think there is a necessity for the establishment of a Commonwealth aviation intelligence group in Australia similar to that which exists under the Transportation Security Administration in the United States.

CHAIRMAN—You need a what?

Mr C. Williams—I suggest that the JCPAA consider recommending the establishment of a Commonwealth aviation intelligence group in Australia similar to that which exists under the Transportation Security Administration in the United States, which is actually part of the old FAA, to be responsible for a range of issues. I will not go through the issues if you want to save time, but I have listed a number of areas where I think that an aviation intelligence group could be very active and very useful. I suggest that it be located within DOTARS, but that would be perhaps subject to further consideration.

In relation to aircraft, the second area, I feel that we should ban duty-free bottles from civilian aircraft passenger cabins, the reason being that a broken bottle makes a very good weapon. I think there are ways around this issue that will not hurt Qantas financially and that will still allow passengers to have duty-free goods. But I think having bottles in aircraft is not a good idea. There are other issues to do with bottles as well. Apparently Qantas has plans to have self-serve drink bars on passenger aircraft; I think that is also not a good idea. At the moment, the cabin crew do have some control over the intake of passengers. Self-serve drink bars could lead to air rage incidents. Also, there is the issue that, for example, a bottle of brandy can quite readily be turned into a Molotov cocktail. I do not think passengers should be permitted to carry bottles, whether they are glass or plastic, containing liquids onto aircraft, because there is the potential for the use of chemicals to make a binary weapon. Also, the kinds of materials contained within a bottle could be hazardous. I am suggesting that there be a prohibition in that area.

It could be useful to have a security buffer zone in aircraft of the first 10 rows from the cockpit, which would basically be frequent flyer passengers, because that would make it more difficult to access the cockpit when the cockpit door is open.

I believe the government needs to review with the US, UK and Israel potential onboard systems to protect civilian aircraft from MANPADs—man-portable air defence systems—when they are transiting higher threat areas, and that applies both to military and civilian aircraft. We do have a project being developed at the moment by DSTO and that should be fast-tracked, but we also need to work with the US, UK and Israel on this issue.

In relation to metal cutlery on planes, I like using metal cutlery myself but I think it presents a danger—and it also appears nonsensical to passengers when they have been screened and had this kind of thing taken off them in the screening process to then be issued with metal cutlery in the passenger cabin. There is an issue with lockers and underseat areas. I believe that those should be searched before passengers board aircraft and I believe that they should be cleared at transit points, so that a person could not leave a device on the aircraft when they get off at a transit point.

In relation to flying staff, cabin crews should meet minimum international security proficiency standards in accordance with ICAO guidelines. They do not have to do that at the present time. I believe that there should be a requirement for all flight crew to attend security awareness training on a regular basis, and that should be audited to ensure that people do attend those sessions. All flight crew and ground staff entering an aircraft should be security screened before boarding, to the same level as passengers.

In relation to airports, new airports and airports undergoing renovation should be required to meet best practice security design requirements, and those would need to be established by DOTARS. Check-in staff should be aware of stress indicators for individuals who are potential hijackers, bearing in mind that an al-Qaeda hijack would need five people, normally. All airside staff should be security screened and they should be required to pass a security background check to five years. That is important because a police check is not going to show you how long a person has a checkable background. It would mean that, say, a person who had a checkable background for three years and had come from Pakistan probably would not be able to work on the airside of an airport. That is an important security measure.

In relation to legislation, there is a need for legislation to compel captains of civilian passenger aircraft to accept air security officers on board. At the moment, they do not have to accept them—although I am not aware of any cases where they have been refused. I think the government also needs to give the ASO program a longer life expectancy to ensure its attractiveness to potential recruits and to ensure staff retention. At present its continued existence is subject to review every 12 to 18 months.

In conclusion, I recognise that a lot of these measures come at a cost, but the alternative is the potential loss of an aircraft and those on board. The loss of an aircraft or deaths at an airport as a result of a reasonably foreseeable violent incident could ultimately be ruinous in terms of litigation against those held responsible for not implementing appropriate security measures. Of course, the cost to the victims' families is not quantifiable. That is a very quick skip-through of what I have written, just picking up on some of the points.

CHAIRMAN—Thank you. You brought up the issue of SAMs and MANPADs, which appeared all over the *The Australian* yesterday.

Mr C. Williams—That was not of my doing, I am afraid. That was a journalist who was putting together an article and I thought it was going to come out later in the piece. It rather pre-empted everything, I am afraid. It was not of my doing, though.

CHAIRMAN—It did do that. In some respects I was a bit disappointed. I thought the photograph on page 4 was a bit over the top. It showed a Qantas plane taking off and a SAM headed towards it. I am not sure we really need to frighten the public that much. I question whether that is necessary in the circumstances where we have had a severe downturn. We interviewed Industry, Science and Tourism the other day about tourists. We have had a severe downturn as a result of September 11, another downturn with 12 October in Bali and another with SARS, and so it goes on. Our export industry in tourism has been hurt badly, and I am not sure that those sorts of headlines and images do anything for aviation security.

Mr C. Williams—I agree with you there. It is a problem with a free media that they will pick up on what they can use to sell papers.

CHAIRMAN—I am not chewing you out. I have no criticism of you whatsoever.

Mr C. Williams—I have tried to be objective on these issues.

CHAIRMAN—I accept that. We respect your position and we respect where you are coming from. I note that yesterday on 666, in responding to that, the Prime Minister commented that he thought that it was right that the threat from MANPADs was greater than the threat of hijack and/or bombs on aircraft. From what reading I have done in study ahead of this inquiry, I would have thought that was not the case. I would appreciate your view. I am not trying to draw a fight with the Prime Minister. It is just that I would have thought that was not true.

Mr C. Williams—I am just trying to think when the last occasion of a bombing on an aeroplane was. I would think it has been some years since there has been a bomb on an aeroplane, particularly a politically motivated one.

CHAIRMAN—It was not that long ago that some very wild people turned aircraft into missiles.

Mr C. Williams—Certainly. The 9/11 attacks were turning aircraft into bombs, yes. But in terms of hijacks, I think the measures taken since 9/11 would make hijacking much more difficult now. Therefore, by comparison, if a terrorist group wanted to have a go at an aircraft, clearly the use of a surface-to-air missile would be an easier or perhaps more attractive option.

CHAIRMAN—I hear you, but DOTARS says that to use a SAM you need intent, capability and technical training. So you need intent and capability plus extensive training.

Mr C. Williams—The capability probably does exist in parts of South-East Asia.

CHAIRMAN—How about domestic Australia, for instance?

Mr C. Williams—Not at all in Australia. I do not think there is any threat to aircraft from surface-to-air missiles in Australia.

CHAIRMAN—Thank you. I am glad to hear you say that, and I will quote you.

Mr JOHN COBB—That is subject to somebody coming into Australia out of South-East Asia?

Mr C. Williams—I cannot exclude it, obviously. There is a possibility of it, but I think it would be fairly unlikely. Why would you have a go at an aircraft when you can wait for the aircraft to come to the area where it is more convenient for you to have a go at it? The area I think it is most likely for there to be an attack of that kind—looking just at Australian aircraft—would probably be Thailand, because we know those systems are available in Indochina. We know that there are people in Thailand with that kind of intent, although we do not know a lot about JI in particular in Thailand. As for the technical issue, my understanding is that the training needed to use these sorts of systems is not particularly much. The SAS people who went into Afghanistan to train Mujaheddin did it in a matter of a couple of hours, so it is not complex.

Mr JOHN COBB—There are only so many ways to fire a gun, yes.

Mr C. Williams—Yes, that is right. You get a lock-on and then you launch. But it does need to be done in daylight hours. If you did it at night, for one thing you would not be able to identify the nationality of the aircraft. The second thing, of course, is that it is a lot easier to get a lock-on during daylight hours.

CHAIRMAN—Identifying the aircraft is an important part of this question. Our understanding from DOTARS is that there are about 900 flights into Bangkok a day, four of which are Qantas flights. So there are four red kangaroos on big tails going in there. The Prime Minister said in his statement on 666 that there were 880 flights—and I would not have a clue which statement was right, but 880 and 900 are not that far apart—with four being Qantas flights. It would take a lot of intent by a terrorist organisation to really harm Qantas and/or Australia for that to occur, wouldn't it?

Mr C. Williams—From their point of view, the desirable targets would be US aircraft first, probably Israeli aircraft second—I do not know whether Israeli aircraft transit Bangkok or not—UK aircraft third and, probably, Australian aircraft fourth. Of those, we would be in the bottom 10 per cent of that quadrant. So I suspect that the chances of our aircraft being targeted are quite low.

CHAIRMAN—If you did a regression analysis, I would have thought the numbers would be almost infinitesimal.

Mr C. Williams—If you take out of that 880 to 900 flights the flights that are actually British, Israeli, US and Australian, you would be down to a much smaller number. I do not know what that would be. If it were 40 aircraft, you are choosing four out of 40, which is a greater risk factor. But, clearly, if you were doing it during the day the big red kangaroo would be an easier thing to see than symbols on most other aircraft. It is a great marketing symbol, but unfortunately it is also a great target.

CHAIRMAN—I am not sure I appreciate that advice!

Mr C. Williams—I am still saying that we are in the lower level of risk here. I do not think it is something that would cause me not to travel through Bangkok, for example.

CHAIRMAN—This committee has had a bit too much excitement in the past two days. We had expected this inquiry to generate interest, but first Mr Clive Williams was quoted in the *The Australian* yesterday and then we woke up this morning and, on our way in to Parliament House, found the ABC broadcasting that Customs, who appeared before us yesterday, had had either mainframes or huge servers stolen out of a secure environment. That has put the sort of negative highlight on this inquiry that we were not looking for. Would you have expected something so bizarre to happen in the Australian context?

Mr C. Williams—No. I think the kind of aviation security incident that is more likely to occur in Australia is the sort of thing that we have seen over the years—which is essentially a single individual, usually mentally unbalanced or stressed, creating an incident on board an aircraft and sometimes trying to take over the aircraft. I do not think it is very likely we will see a group try to hijack an aeroplane in Australia.

CHAIRMAN—I meant the hijacking of the computer.

Mr C. Williams—Cyber issues are another area of concern more generally, from a security perspective. It has been a concern internationally that somebody might hack in and be able to take over the control systems at an airport or that sort of thing. That would, of course, be very much a concern because it could cause havoc with air traffic. That will depend very much on whether there is a stand-alone system at an airport that is isolated from external contact. I do not know enough about them, but I would hope that most of those sorts of systems are stand-alone systems.

CHAIRMAN—We do not know what it was yet, either. We have not long ago finished having public hearings for a several months inquiry into IT security in the Commonwealth, and I cannot

recall any of the respondents or any of those who appeared as witnesses before the committee mentioning the possibility of theft of a mainframe.

Mr C. Williams—It is unusual. Normally we lose laptops, not mainframes.

CHAIRMAN—I can understand losing laptops and people stealing laptops. I am pretty good at losing cameras. But I find it almost incomprehensible that somebody could walk in and steal a big computer. Do you agree with that?

Mr C. Williams—Yes; I am a bit staggered by it as well.

CHAIRMAN—I would hope that, as a result, it will never happen again.

Mr C. Williams—Yes. Once one of these things happens, you hope that safeguards are then put in place to prevent a recurrence.

CHAIRMAN—The DSTO is doing research on MANPADs, or deterrents.

Mr C. Williams—I understand that it is called Merlin and is a laser based countersystem. As you probably know, the military have flare systems which are 90 per cent effective, but I do not think they can be used on civilian aircraft, because they can cause fires both on aircraft and on the ground. So for that reason I do not think it is practical. You are probably looking most likely at a laser based system, which is what Merlin is. I think that is probably the way the US research will go—for a laser based system. An important consideration is that it is a low-cost system, because obviously you do not want to pass on too many costs to airlines if they are going to be paying for it. The aim of a laser system is that it burns out the seeker system of an incoming missile.

CHAIRMAN—Even at low level and low speeds?

Mr C. Williams—Yes. Most of these missile systems have self-destructs. Once the seeker is burnt out, the missile will self-destruct. That is the aim of this system. There are comparable military systems to this, but obviously it would be attractive to have a relatively low-cost Australian system that could be fitted on to aircraft that transit high-risk areas—and I am thinking about military and civilian aircraft. It does not need to be fitted to the whole Qantas fleet, for example. If you had a system that was transferable from one aircraft to another, you could reduce the number you actually needed to buy in the first place. That might be an option as well.

CHAIRMAN—You will probably agree with me when I say this: in talking about this issue, I think it is important that we all realise we do so not in the context of domestic aviation but in the context of international flights—flights that either originate overseas and are destined for Australia or are from Australia to overseas destinations. We are not talking about Australian domestic air travel.

Mr C. Williams—Yes. We know there is a reasonably good quality of screening at major airports in Australia and, therefore, the level of risk is much lower here than it would be going

through an environment where people, as you say, do have an intent against us and may have systems they can use against us—not only surface-to-air missiles but other systems as well.

CHAIRMAN—Our look at the borders over the last few years with both Coastwatch and AQIS would tend to tell us that it would be pretty hard to smuggle a SAM into Australia, unless you were to put it on a yacht, sail it into the Northern Territory and walk it down a track—except that a pastoralist would be bound to see you.

Mr C. Williams—It is possible to bring one in, but there would be a degree of difficulty that does not exist in operating in other parts of the world. I think the same thing would apply with the United States and the UK: it would be difficult to get one of those systems into a position where you could use it on the ground. That is why it looks more likely to me that you would use one of those systems in an overseas location.

Mr JOHN COBB—I would have thought it would be very easy to use one in Australia; it would be the getting away with it that would be the difficulty, compared with some other places, wouldn't it?

Mr C. Williams—It is actually bringing it into the country that I think would be quite difficult. Naturally it is not impossible, but I think it would be quite difficult to bring into the country. As our screening processes for containers improve, that would make it more difficult still. You would have to hope also that Intelligence would be able to give you a tip-off in this area; that is, if people have been purchasing these systems and are trying to bring them into Australia, you would get some sort of tip-off beforehand.

Mr JOHN COBB—We have a very big north coast; I have been up there. That is the way I would have thought they would do it. You have mentioned stress indicators, and I am not sure that I understood what you were saying. Did you mean that there should be stress indicators you can run on all the passengers? Is that what you meant?

Mr C. Williams—No. Customs, for example, when looking for people carrying drugs, will look for stress indicators such as perspiration, licking of the lips, looking around a lot and shifting of position—people who apparently are nervous.

Mr JOHN COBB—I can understand why you would want to do it, but is it in connection with passengers either in the aircraft or going through Customs?

Mr C. Williams—No. This is actually before that; they are observed when they are in the boarding lounge area. If there are people there who appear to be—

Mr JOHN COBB—Did you mean that this be done by observation?

Mr C. Williams—Yes, just by observation. I was not thinking of any systems in that regard.

Mr JOHN COBB—Did I understand you to say that captains of civilian aircraft are not bound by federal law and they do not have to accept ASOs?

Mr C. Williams—Yes, that is right. The captain can take the decision that he does not want an ASO on board. I have not heard of that happening, but it is a concern that a captain could say, 'No, I don't want them on board—end of story.'

Mr JOHN COBB—I would agree. You mentioned a lot of things—which sounded to me not terribly expensive—that can be done. Have you passed those on to DOTARS or whatever the relevant agency is?

Mr C. Williams—No, I thought I would talk to you about it beforehand. I did not want to raise it with others. I have spoken to people about some of these issues. For example, I did check to see whether there is or has been any aviation intelligence body since I left the intelligence community—and there is not. I wanted to be sure of my ground in some of these areas.

Mr JOHN COBB—I notice you are with the Strategic and Defence Studies Centre at the ANU. Are airports and aviation safety a particular focus within that centre?

Mr C. Williams—No. I work on terrorism issues, but I also provide training in aviation security issues. When I travel I quite often meet with overseas agencies like the Transportation Security Administration and go on security tours of airports so that I can see what the latest technologies are that they are using—that sort of thing.

Mr JOHN COBB—As the chairman mentioned, the main focus is obviously on the major airports where the big planes and jets fly in, but we are also charged with looking at security at regional airports. Do you have a view about that? If you do, do you agree with what is currently being looked at? Do you have a view about security at regional airports—for example, Albury or Dubbo? Obviously, we are talking about the bigger ones.

Mr C. Williams—I think the most resources obviously need to go to airports that are the major concern—those dealing with jets and overseas traffic. Therefore, the screening resources need to be best in those areas. Then it is really an issue of how far your resources will stretch to smaller airports. I have been through quite a few smaller airports in the United States where there is no screening but, when you get to a major airport like Los Angeles International, you do go through a screening process. In terms of comparing Australia with the United States, I would say that we have a comparable level of security.

CHAIRMAN—At the beginning of your presentation you talked about an aviation intelligence organisation similar to what is established in the United States. You said you thought it could possibly be located within DOTARS. Are you proposing that it simply be used for gathering and filtering intelligence information?

Mr C. Williams—I will very quickly run through the areas I think that such a body should concentrate on. I think it should advise Australian civil aviation on an ongoing basis of the nature of the security threat within Australia and externally; undertake assessments of the security situation at overseas airports used by Australian carriers; and provide input to contingency planning for Australian air evacuation within South-East Asia and the South West Pacific. I think we were fortunate that Bali was only 2½ hours from Darwin, and we actually had ADF people on the ground very shortly afterwards, which was very fortunate for us. But we do need to do better contingency planning for contingencies elsewhere within the region.

Such a body could also provide advice on civil aviation issues to the SAS, because they need to know about, for example, changes to design internally in aircraft. They also need to know about any change issues with overseas airports, because SAS does have a counter-hijack role which might take it overseas. Such a body would liaise with similar intelligence bodies overseas—say, for example, the one at TSA; provide input to government intelligence assessments and travel advisories where these relate to aviation; and provide expert comment to the media when needed and appropriate. There is a range of areas where I think it would provide a service.

The reality is that, in many cases, unless you have an agency comparable to one in the United States, you do not get a lot of information out of them. For example, our Defence Intelligence Organisation gets a lot of information from the United States Defense Intelligence Agency. If you do not have a body comparable to an American one, it is much harder to get the information. I think that such a body would be able to tap into information that is provided in the aviation system in the United States more easily than existing organisations can.

CHAIRMAN—Do you believe that, as you have just defined, it needs to be more narrowly an information organisation? Or need it have some outputs other than just information and some outcomes?

Mr C. Williams—It would actually be doing intelligence assessments—

CHAIRMAN—No, a coordination role, for instance. Are you familiar with the national surveillance centre that operates under Coastwatch?

Mr C. Williams—Yes.

CHAIRMAN—There are a huge number of organisational inputs that feed into that centre. From that centre come real outputs—directions to aircraft and vessels and personnel on the ground, if necessary. My view is that it performs a vital national service in that respect. You don't envisage that such an organisation could or should operate in this area of aviation security?

Mr C. Williams—I was not making a judgment about where it should go; I thought DOTARS was—

CHAIRMAN—No, not where; I was talking about the fact that it has real outputs as well as just information.

Mr C. Williams—One thing we are lacking is a networked system. That is a weakness on the part of the way we are set up at the moment. Traditionally, we thought of national security as involving Defence and the intelligence community and so on, and now Immigration and Customs and some of these other agencies are brought into that. I certainly think DOTARS should be brought into that if it is hosting an intelligence group like that. The information flow should certainly be between the Coastal Surveillance Centre and a body like this—it has a role to play in all of this.

CHAIRMAN—Would you perhaps have a look at what Coastwatch does in that respect if you are not intimately familiar with it and perhaps come back and tell the committee what you think about that as a model in this area of proposed control?

Mr C. Williams—Yes.

CHAIRMAN—I do not know whether it is right or not; I am just asking that some people that are thinking hard about this issue on a broad scale give some thought to direction and what might work best and recognise that, as in coastal surveillance, in this area of national security there are a terrible number of agencies involved, with very few memoranda of understanding between them and no common, central control centre, if you will.

For a long time I was in the industrial instrumentation process control industry, and we started out with individual controls on each individual control loop—a flow loop, a temporary loop, a pressure loop or a level loop. Then we concentrated some of those in areas of a plant, so you had a control panel and it operated several different control loops. Then we got down to the concept of the central control room and we took all the signals from all over the plant and brought them into a central room, manipulated the data and sent our control signals to a control valve operating from the central control room—now we do it with computers. That, in essence, is what happens with the National Surveillance Centre: instead of a whole bunch of individual loops, or even individual groups of loops, there is one single control room. Give some thought to it, would you, and come back to us?

Mr C. Williams—As I say, I think an aviation intelligence body would link in very well to the US one. I take your point about the Surveillance Centre and all of that, and it should certainly be linked to that, but what we are talking about is something more extensive than that, because it will have overseas responsibilities and will need to liaise with similar organisations, probably in South-East Asian countries and elsewhere as well. It has got an international role, really.

What I envisage is that you would have people who have an intelligence background and an aviation background, so former RAAF intelligence officers would be appropriate for that. They also have to be aviation industry sensitive so that they do not come out with recommendations or assessments which are going to cost the aviation industry disproportionate amounts of money because, clearly, we have to think about the cost to passengers and the competitiveness of Qantas in these areas as well.

Mr JOHN COBB—To return to the regional side of things, currently when you fly into Sydney, as I do a lot, you can get to Sydney without going through screening but you cannot board a plane in Sydney without going through screening. Given the information that we have available at the moment, do you see that as being sufficient security?

Mr C. Williams—Yes, I think so. If you ended up, as I know is the situation in some airports overseas where you have a mingling of passengers that are coming in from regional airports with people who are going off on international flights—

Mr JOHN COBB—That does not happen.

Mr C. Williams—that is unacceptable. There has to be obviously a division between those people and a system that prevents them from skipping from one side to the other. As far as I am aware, in Sydney you cannot very readily skip from one side to the other.

Mr JOHN COBB—You would be going somewhere illegal to do it.

Mr C. Williams—Yes, that is right.

CHAIRMAN—You talked about a security buffer zone on aircraft. Is that between ticket classes?

Mr C. Williams—I was thinking that if you are travelling on a two-deck aeroplane, you have business class in the upper cabin there—

CHAIRMAN—And down.

Mr C. Williams—Yes, but the cockpit is in the upper cabin.

CHAIRMAN—Yes, fair enough.

Mr C. Williams—So if you said that people in the upper lounge area—which I do not think would actually have 10 rows, but somebody else would know better than I do on that—all had to be frequent flyers, that gives you a measure of security: it makes it more difficult for somebody to come up and access the cockpit.

CHAIRMAN—Are you saying a frequent flyer would not—

Mr C. Williams—Generally speaking, hijackers are trying to obscure their identity and obscure the fact that, even if they are regular travellers, they travel regularly and they often travel under different names anyway, so I would suspect they would avoid being grouped as frequent flyers because it would give you a window on their movements. So therefore I am suggesting that it is a way that an airline could quite easily, at no cost, build in a little bit more security in this area.

CHAIRMAN—Thank you once again. We appreciate your continuing interest in providing the committee with information in this vital area. When you finally see the transcript, give some thought to what I have asked you to have a look at.

[3.23 p.m.]

LOCKET, Miss Carol, Occupational Health and Safety Convenor, Domestic and Regional Division, Flight Attendants Association of Australia

MACLEAN, Mr Guy William, Manager, Safety and Regulatory Affairs, International Division, Flight Attendants Association of Australia

CHAIRMAN—I welcome the representatives from the Flight Attendants Association of Australia to today's hearing. Thank you for coming. You supplied a submission but we did not have to time to include it; you were a bit late. Do you have a very brief opening statement?

Mr Maclean—Yes, and we understand that at this time on Friday afternoon, we had better make it brief.

CHAIRMAN—Or we are going to turn into pumpkins.

Mr Maclean—Indeed. I will say that we speak as a united presentation today on behalf of the Flight Attendants Association of Australia in general—both divisions are presenting a joint submission and presentation to the committee.

To be brief in that case, I will discuss two broad areas of our submission rather than going through all the dot points. However, we would be pleased to discuss any of the points we have made as the committee sees fit. We will talk broadly about consultation issues that impact on safety and security in aviation, and we will talk about the commercial impact we see on safety outcomes within aviation. Before I start, giving you the context of our presentation may be useful. We have a significant luxury, and that is that we have not developed any of the multitude of systems, provisions, procedures and mechanisms that we have heard about over the last two days. We are a consumer of them, and in that sense we are not required to defend them. All we can do is quite simply tell you, from the perspective of the aviation worker—the end user of these systems—whether they work. That is the value that we can give to the inquiry.

I will also briefly outline the role of a cabin crew member because, in contrast to the general marketing focus of our role, we see the role of a cabin crew member to be clearly a safety and security role. Cabin crew perform that role under a mandate from annex 6 of ICAO, and they are required to be on board aircraft to perform, in the words of ICAO, 'safety and security' functions—safety functions being outlined in chapter 12 of annex 6 and security in chapter 13. Much of what we will say will discuss the impact that the current environment has on our ability to perform those mandated functions. In relation to that mandated role, we have heard significant discussion regarding the need for consultation between industry and government. We heard the Australian Federal Police and the Customs Service say that their various systems benefited from cooperation and coordination between parties. We have not yet heard anyone include the people—the human beings, the system operators—who have to implement the full range of security and safety mechanisms. We represent the people who will actually do those tasks. I note Customs's belated acknowledgment that perhaps the people were more important than they initially gave me the impression they felt they were.

We say in relation to cabin crew that no security system anywhere is going to be 100 per cent effective and that security systems will be breached from time to time—very infrequently we certainly admit and are pleased about. But the people whom I am speaking on behalf of today spend their entire working lives on board aircraft. Their safety and security is indistinguishable from that of the general travelling public. The cabin crew have a specialist cabin safety knowledge about their area of operations. The procedures and mechanisms that are developed have an intimate impact on them. As I said, they carry out those duties, yet we see time and again that in the vast majority of cases cabin crew are not consulted when systems are evolved or developed.

A good example would be the recent development of the Aviation Transport Security Bill 2003. Despite our intimate knowledge of the area which it covers in the aircraft environment and the impact it will have upon us, we received no consultation whatsoever. I have raised that with the department, and we have an undertaking from the inquiry into that bill that they will consult us in the development of the regulations that will stem from that bill. We have put quite a lot of effort into developing relationships with the department, the operators and the government, and to be fair many of those relationships did not exist previously. I am hopeful that next time we will be considered more vital to this process.

We can add a significant amount of value to these processes, and I point to other programs, such as the biometric program—which we had a good consultation mechanism put into, and I think we added significant value to that—and, probably more importantly, the ASO program. After initially being overlooked, it was then recognised by the program's operational planners and managers that we had some specialist knowledge, so we were given a very close consultative opportunity to contribute that and add value to that program. I believe we have, and I believe that is the way forward.

In the current much evolved climate since September 11 it is no longer practical to simply issue instructions to the aviation workers, such as cabin crew, for compliance. The principle or philosophy which in my view has been fairly clear from all the witnesses before this committee in the last two days is one of inclusion—and I think, Mr Chairman, in your opening statement to this committee yesterday you highlighted that. The Minister for Transport and Regional Services, in his second reading speech on the aviation security bill, also mentioned the fact that we must all be included in aviation safety. There is a way to elicit that inclusion, and we must all contribute. I do not think that a single dimensional instruction that cabin crew or aviation workers just follow the rules and do what they are told elicits anywhere near the contribution which we need in the new environment. We stand ready to contribute.

Other factors are impacting on our ability to conduct our mandated security and safety obligations. In this context I note organisational fragmentation is an increasing feature of the aviation industry. We do not want to be overly critical of the airlines in this respect, because we see in large part they are reacting to government policy to allow levels of deregulation, which this association believes drive that kind of organisational fragmentation by putting an excessively high focus or necessity on commercial factors. This kind of fragmentation means that many of the core functions in producing an aviation service are now being outsourced, and in many cases those persons have only an indirect relationship with the core operation.

Airlines and the aviation system operate in a safety culture. The British have coined a term 'the virtual airline' to reflect the UK's experience of very high levels of organisational fragmentation. In our view, in relation to safety culture, a virtual airline would have a virtual safety culture and a virtual security culture. Yesterday we heard the ANAO referring to a security culture and the fact that they would like to see the safety culture extend to the security culture. I agree completely but in our view, due to the economic framework which aviation services are developed in and operate under, the current trend is sadly driving us away from that outcome, not towards it. We also think of human factors for all participants in the security section. My personal background is as a human factors specialist. Ms Grierson mentioned human factors. That rationale should also be applied to all systems.

CHAIRMAN—Thank you for that, and thank you for sitting through two days worth of public hearings. You have been patient indeed. At the front of our briefing papers is a list of incidents in the air in Australia over the last few years, and the flight attendants, whom you represent, certainly feature heavily in securing our security in that respect. We compliment the attendants in that regard. I will take you slightly to task on the last bit of what you said—that we have perhaps deregulated too far. Ansett had a huge staff, but Ansett has gone, and it has gone forever. There are a lot of chapter 11 airlines in the United States, but other bigger airlines that flew out of the United States no longer exist. You know that competition is heavy and if we are not competitive then somebody else will be doing it for us, so we have to be a little careful, don't we? It is like the argument about regional airlines, and I am sure you have some comment about that.

We have heard, as you know, that there may be a trade-off between having security at small regional airports and having regional airports at all, because if we force them to have too much security and very expensive screening systems then no aircraft will fly, the public will not have access to the airports and people will not have jobs. Do you believe that the Qantas trial of the face recognition system is going well?

Mr Maclean—Yes, I do. As I mentioned, we had quite an involved consultation for the start-up of that system. In the international division of the association—because it does not apply to my domestic colleagues—it is currently being used in Sydney. We looked at it very carefully. I attended meetings with the manufacturers and Customs. We initially had significant privacy issues and we needed to see how they were addressed. Through our support of that initiative, we have seen figures of somewhere over 96 per cent of Qantas long-haul cabin crew, tech crew and pilots signing up to participate in the trial. They now use that technology comfortably and enthusiastically; they really like it. Facial recognition technology is our preference, because it is much less invasive. We note that during the recent SARS epidemic, for example, it was a factor that made us comfortable in that we did not need to touch the machine or have anyone touch us.

There are significant privacy implications but, as I understand it, this facial recognition technology in the current trial does not interrogate third-party databases. Basically, it is saying that the person standing in front of the machine is the person in the passport that is being presented to the machine. It is not going away and checking if you have unpaid speeding fines or something else. Should the thing evolve further into a database that starts doing those sorts of things, we would be very interested to pursue those and understand very clearly what those dimensions are.

CHAIRMAN—You said you are fully on board with air security officers now. Do you approve of their being armed?

Mr Maclean—We believe that the air security officers on board our aircraft are a vital asset. They are highly trained professionals and we are happy with them being there.

CHAIRMAN—Are you familiar with Taser?

Mr Maclean—Yes, I am familiar with it as a concept.

CHAIRMAN—Do you have a view?

Mr Maclean—The implication of your question is: do we feel it would be appropriate for cabin crew to be armed with a nonlethal weapon such as this? This is a deep and very complex issue which we will seek to evaluate very carefully as a philosophy before we take a step down that road. The context is that the flight deck door is locked: you cannot go in and you cannot go out. In an emergency situation, the aircraft goes into lock down. The old days of the captain coming out and reading the riot act to disorderly passengers are finished. The cabin crew are completely responsible. We have aircraft getting bigger and bigger whilst the flight deck crew is shrinking to two. We have two pilots on the majority of the world's airlines. We have passenger cabins simultaneously getting larger and larger. We have higher numbers of people on the aircraft. We are moving towards ultra- or long-range flying, and we have locked cockpit doors. The cabin crew have to deal with any issues that arise in that cabin. In that context, in a severe hijack situation an air security officer could be the difference between life and death. We see them as providing a potentially lifesaving response. In that kind of extreme situation, a Taser might be a device that could save our lives and the passengers' lives.

Mr JOHN COBB—Like the chairman, I would like to thank you for the interest you have taken in the review. How comprehensive, extensive or different has the training you have received in obvious areas been in the last two years compared to what happened before?

Mr Maclean—There was not an immediate response.

Mr JOHN COBB—I mean the on-board response.

Mr Maclean—I am differentiating in our presentation now. We are talking about the safety and security role of cabin crew. We obviously provide a very important service role as well, but our comments relate to the safety and security role, which we see as the main role. We have had quite a bit of discussion with the major operators. A cabin crew training program specifically addressing hijacking and security issues is now in force. It took some time to get that training program in place; it was a big and complex issue. We were able to participate in the development of the program. The feedback we are getting from the crew is that they love it. They are saying: 'It's fantastic. This is what we've needed for so long.' They are very pleased to be finally getting that training, to enable them to protect the lives of the people who are completely under their professional care whilst an aircraft is airborne.

Miss Locket—It gives them practical skills—far more than the theory. The emphasis has changed since September 11. Prior to that, there was much more of a passive role in an attempted hijack. Now if the cabin crew do not react, the passengers certainly will.

Mr JOHN COBB—With good reason.

CHAIRMAN—We have noticed that, haven't we? We noticed that on the flight from Melbourne to Tasmania, both the cabin crew and the passengers reacted in tandem—and very well.

Mr Maclean—We cannot rely on that. I am aware of two instances in the US where a passenger has attempted to kick in a flight deck door, the cabin crew have called for assistance from the passengers and they have not assisted. Whilst I imagine that, in the majority of cases, there would be a lot of willing assistants, we do not consider that to be standard.

Mr JOHN COBB—You do not rely on it?

Mr Maclean—We do not rely on it.

CHAIRMAN—Mr Maclean, may I remind you that this is Australia?

Mr Maclean—Indeed.

CHAIRMAN—That was a good point, wasn't it?

Mr Maclean—I would point out that, with a large international airline like Qantas, their customer base is less and less Australian. I do not know the percentages, but I would be surprised if Australians are even in the majority any more. We have a range of nationalities. Those aircraft operate over the entire globe and you could not rely on the fact that you had a lot of gung-ho Aussies to stand by you and help.

Mr JOHN COBB—You mentioned that the systems we have been hearing about for the past couple of days—most of which I would have thought, off the top of my head, do not come across your desk, so to speak—deal with people before they get on board, or they are more about systems than they are about dealing with people. By and large, do you have reasonable confidence in the way things are going at the moment? Do you have an area of major concern?

Mr Maclean—In terms of the professionalism of those who address security in the industry, I think they are extraordinarily well qualified.

Mr JOHN COBB—Competent?

Mr Maclean—Competent, yes. For example, I have some reasonably regular dealings with the Qantas security and investigation service. My impression is that they provide a very high-level service which is probably as good as, or better than, any in the world. Our issue is not with the fact that they do not know what they are doing. I refer not only to the airlines but also to the government departments—for example, in the Civil Aviation Safety Authority there is no cabin safety specialist within the standards branch; cabin safety specialists are only in the compliance

branch. You must consider that, due to fairly high levels of commercial pressure, we now have airlines seeking to introduce product innovation into the aircraft cabin more quickly than in almost any other area of aviation.

Mr JOHN COBB—What do you mean by 'introducing product innovation into the aircraft cabin'?

Mr Maclean—Airlines are a non-differentiated product. As they compete against each other very heavily, they need to differentiate their product from that of their competitors.

Mr JOHN COBB—You mean faster food and better liquor?

Mr Maclean—More service, yes. It is better quality of product—it is referred to generically as product—and higher levels of service. It is often very difficult for the cabin crew to supply these higher product levels because, simultaneously with the offering of higher product levels, we see a very strong cost focus which is driving us towards minimum crew numbers. That has a service implication—the airlines manage that as they see fit, obviously—but it also has a security implication. Airlines seek to operate at the lowest possible labour costs, and cabin operations are not excluded from that. As they address the high levels of competition, they have a lot of innovations and they want these generally in the cabin of an aircraft more quickly than innovation is required in any other area of aviation, I believe. Quite often the regulatory mechanisms and the security frameworks do not directly address some very new and innovative ideas. Now, with DOTARS having no cabin safety specialist experience on their staff—

Mr JOHN COBB—So the ideas are in front of the security that goes with them?

Mr Maclean—I believe so, yes, and CASA do not have the expertise. Another group, the Aviation Safety Forum, was set up by the government to advise the CASA board. No member of that has cabin safety specialist experience either. This is why we seek to have input into this process, because we know about these things.

CHAIRMAN—Thank you for giving us that advice. You heard Mr Clive Williams suggest that we ban duty-free bottles on aircraft, that we ban self-service drink bars on aircraft and that we ban bottles containing liquid on aircraft. Do you agree or disagree?

Mr Maclean—In a perfect world, and in the highest security context, those steps would be taken. I would personally like to see bottles banned from aircraft, but I think that would be a very difficult step to take, and not selling duty-free to passengers on departure would be a difficult step to implement. As a philosophy, I think it would be quite a good one. With respect to passengers carrying bottles onto an aircraft, we would certainly like to see—and we pointed this out in our submission—bottles of liquid examined and identified. A fire specialist has informed me that with a one-litre bottle of accelerant, rather than water, you could start a fire that would probably be impossible to put out, and you would have noted that people with bottles get on aircraft all the time. I would like to see that as a standard screening response.

Mr JOHN COBB—Miss Locket, did you say you are from the regional side?

Miss Locket—Domestic and regional.

Mr JOHN COBB—Do you have any comment at all from the regional, as against the international, side of this?

Miss Locket—Certainly from the domestic security side, we would like to see all ground staff that have access air side receive the same security screening that cabin crew do. Baggage handlers, cleaners, caterers—

Mr JOHN COBB—That is not happening now?

Miss Locket—are not screened on a daily basis when they come to work in the same way that cabin crew are, and yet they have access to the aircraft.

Mr Maclean—In many cases that access is after an aircraft has been declared sterile and security checked by its crew.

Mr JOHN COBB—I take your point.

CHAIRMAN—We are both going to turn into pumpkins, because we have aircraft to go to. Is it the wish of the committee that the additional submission by Mr Clive Williams, dated 5 September 2003, be accepted as evidence and authorised for publication as submission No. 35? There being no objection, it is so ordered. I thank the witnesses, those who attended the hearings, the secretariat staff, the media for their cooperation, my good colleague Dr John Carter, my colleagues on the committee and, last but not least, as always, God bless Hansard.

Resolved (on motion by **Mr Cobb**):

That this committee authorises publication, including publication on the parliamentary database, of the proof transcript of the evidence given before it at public hearing this day.

Committee adjourned at 3.48 p.m.