COMMONWEALTH OF AUSTRALIA

Proof Committee Hansard

JOINT COMMITTEE OF PUBLIC ACCOUNTS AND AUDIT

Reference: Review of aviation security in Australia

TUESDAY, 21 OCTOBER 2003

MELBOURNE

BY AUTHORITY OF THE PARLIAMENT

[PROOF COPY]

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://parlinfoweb.aph.gov.au

JOINT COMMITTEE OF PUBLIC ACCOUNTS AND AUDIT

Tuesday, 21 October 2003

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

Senators and members in attendance: Senators Watson and Mr Charles *(Chairman)*, Ms Grierson, Ms King and Ms Plibersek *(Acting Chair)*

Terms of reference for the inquiry:

To inquire into and report on:

(a) regulation of aviation security b 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 9.40 a.m.

CHAIRMAN—The Joint Committee of Public Accounts and Audit will now commence taking evidence, as provided for by the Public Accounts and Audit Committee Act 1951, for its review of aviation security in Australia. I welcome everyone here this morning to the committee's third public hearing. The focus of the first part of the hearing will be on security arrangements at airports, with the appearance of the management of Melbourne and Launceston Airports and the Australian Airports Association.

The committee has received conflicting evidence concerning the security risks at regional airports and the level of threats posed by light aircraft. Some say the risk is significant, yet others say the risk is lower than at major airports and lower than the threats posed by jet aircraft. Indeed, other day-to-day activities, such as driving across major bridges, are just as likely to bring one into contact with a 'terrorist event'?

Increasing security at airports will undoubtedly cause delays and inconvenience to passengers. 'Rage incidents' often arise when citizens act out their frustrations. The question is whether increased security will increase incidents of 'airport rage'. This is a concern of the Australian Services Union, which will be appearing this morning.

During this hearing the committee will begin receiving evidence from various providers of security technology and consultancy services. Witnesses appearing today have variously suggested the installation of flight deck security doors and video-monitoring devices in aircraft, the use of a comprehensive security management program and the potential use of profiling frequent flier passengers. The increasing intrusiveness of security related information collected about the travelling public raises privacy issues. Phrases have been used such as the need for privacy to be 'sympathetically compromised' in the event of any increase in threat levels. Yet does the current level of threat facing the aviation industry justify inroads into privacy resulting from the introduction of techniques such as passenger profiling?

The public hearing phase of the inquiry will continue with a further hearing scheduled for Brisbane on Wednesday, 15 November and a final wrap-up hearing in Canberra on Monday, 1 December. Before commencing, 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.

Finally, 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 this committee statement are available from secretariat staff.

[9.43 a.m.]

GRAHAM, Ms Pamela Margaret, Manager, Operations, Melbourne Airport, Australian Pacific Airports Corporation (APAC)

CHAIRMAN—I welcome the representative of the Australian Pacific Airports Corporation to today's hearing. We have received your submission, for which we thank you. Do you have a brief opening statement?

Ms Graham—Yes. Firstly, may I apologise on behalf of Chris Barlow, who is our chief executive officer. Chris is very sick today and has just returned from the UK. He was very keen to appear at this hearing, due to his long background in operations and security at Heathrow and other UK airports in his capacity at the British Airports Authority, where he had responsibility for various aspects of security during a long period of IRA threat and Lockerbie and so forth. He asked whether it would be at all possible for him to appear at another hearing at some stage.

CHAIRMAN—I am confident that we can arrange that.

Ms Graham—Thank you.

CHAIRMAN—He will probably have to fly!

Ms Graham—He is quite used to flying; there is no problem there.

CHAIRMAN—I am pleased to hear that.

Ms Graham—We believe the general management and regulation of aviation security in Australia today to be quite effective. We noted in the submission: 'If it ain't broke, why fix it?' That is generally our position. We believe that the department is heading in the right direction with the new regulations that are currently before the parliament. We believe that they are moving in the right direction with implementing the ANAO recommendations of becoming more systems or outcomes based in security. We think it is essential that DOTARS remain the leader and the aviation security regulator in Australia. It understands the airport business very well, it has the broad picture in its air transport policy role and it is the right organisation to bring all the other participants in security together and to show leadership in that. We also think it is very important for the department, as the regulator and with the access to intelligence, to be the key driver in assessing risk and setting the standards in security nationally.

Finally, we think that during this period of heightened awareness in aviation security, with intense media scrutiny of any incidents that occur, it is important not to have knee-jerk reactions to particular incidents but to keep focused on security outcomes and the right security rather than on the public perception reaction. We, as the airport, accept that we have accountability for the overall coordination of airport security at the airport, but we obviously need support to ensure that all the other users of the airport and all the other tenants also comply with requirements and that we have some teeth to make that actually occur. That is broadly all I want to say at this stage.

CHAIRMAN—Thank you. If your boss feels as bad as I do, I understand why he is not here—and I probably will not be here for very long myself. We have heard that for there to be a major terrorism incident takes three components. The first is intent, the second is capability and the third is training in the use of whatever devices you use to create the incident. Do you believe we have overreacted to September 11?

Ms Graham—I think our initial response to September 11 was very good in terms of the speed at which we were able to implement additional security measures. I think we have almost the right balance at the moment, but I think there is always the danger that, if you have too many incidents, you are going to get a public reaction and therefore the tendency to try to put in security that perhaps is not going to add any benefit to the current regime.

CHAIRMAN—We have heard evidence of air rage on the ground, and later on today we will talk to people about that. Do any of your personnel have problems in the airport environment itself when they come in contact with the flying public?

Ms Graham—In terms of security it would mostly be with contractors—our contractors that manage the screening contract and the Australian Protective Service. So, yes, they do come into contact with passengers who may not always appreciate the benefits of the security that is being offered. I am not going to go into all of them but there are some measures at the screening point that could be argued really generate the right outcome. There have been some measures introduced as a result of September 11 that relate to various cutting implements and so on that you would have to say generate not much benefit and can generate a fair bit of angst with the travelling public at the same time.

Ms PLIBERSEK—You mean things like nail clippers?

Ms Graham—Yes, that sort of thing. That is right. You would have to ask what real threat is posed by that in relation to other things that can be carried on board the aircraft and in relation to other things that people can do on board the aircraft. Those sorts of measures are perhaps not the best suited. But generally the public has been relatively receptive to a number of security measures. There have been some recent measures introduced with explosive trace detection that have been quite well accepted by the public. We also note that in conducting exercises at the airport—such as evacuation exercises where the public might have to evacuate the terminal, and it is just an exercise—we get a very good response now. Probably three years ago we would have got a very adverse response. So in that respect the public has taken on board the need for better security.

CHAIRMAN—At the public hearing in Sydney, we heard some evidence of some people's concerns—I do not want to overemphasise it but there was some evidence of some people's concern—about the unregulated part of the aviation industry, particularly with regard to small regional airports and GA aircraft. You have GA aircraft flying into Melbourne airport. The government have clearly said that their concerns are about large jets with huge fuel loads and large numbers of people. Do you have concerns about the GA industry and the thousands of small unregulated aircraft and places where aircraft can take off and land?

Ms Graham—There is a lot of debate about the smaller aircraft and what sort of threat they pose. I would have to say that on balance we would support the view that obviously the high fuel

capacity aircraft are a much greater risk. At Melbourne we also have not focused on it a great deal because we do not have a very large number of GA operations into Melbourne at all. There are very minimal operations. So there are no real GA aircraft parked in what you would describe as our main apron area where our large aircraft are parked at all. We do not consider it to be a high risk for Melbourne in relation to what other things could be.

CHAIRMAN—I suppose it would be irresponsible of me to be provocative but that small single engine aircraft in Miami that flew into the building did not seem to have caused a lot of problems except to kill the pilot and make a mess of the building, as I recall, but if a small aircraft which took off from anywhere in Australia flew into your jurisdiction you could not stop that aircraft from flying into your control tower, could you?

Ms Graham—No, not without great difficulty. That is right. But you could also argue that that aircraft could be flown into a number of structures or pieces of infrastructure. It is not necessarily going to be more of a threat to the airport than a number of other pieces of infrastructure.

CHAIRMAN—The Arts Centre? The Exhibition Building?

Ms Graham—Westgate Bridge. Security is never going to be absolutely failsafe. There are other threats to aviation security that possibly are much greater than that and still quite difficult to control.

Ms PLIBERSEK—You mention in your submission that you think DOTARS is the appropriate body to oversee security because they have the intelligence to work out what the actual threats are. Are you confident of that?

Ms Graham—I am very confident that the department is the most appropriate organisation to bring together a wide range of expertise that enables it to be the leader in that area. Intelligence is one, but so is their broad understanding of the airport business, their general air transport policy involvement and their long experience in the area. Yes, I am confident that they do get the intelligence. What is happening now and what has been happening over the last few months is that the department and the Attorney-General's Department are bringing together almost what you would call a road show on intelligence. So we feel that we are being briefed quite regularly on what is happening—probably better than we have been in the past.

Ms PLIBERSEK—So you feel that some of that intelligence is being passed on to you for you to improve your systems?

Ms Graham—Yes, definitely. We have had probably three briefings in the last few months on the latest intelligence and threat level. But I still have to come back to the original point that we believe that the department is still in the best position to establish standards overall. I do not believe that every airport necessarily should be establishing its own standards. Certainly you do your own risk assessments that may be appropriate locally for you but still the department must take that role in risk assessment and setting the standards.

Ms PLIBERSEK—Would you say that you have changed any of your operations due to the intelligence briefings that you have had?

Ms Graham—No, not at this stage.

Ms PLIBERSEK—What changes have you made since September 11?

Ms Graham—There have been a number of changes that have been introduced by the department under their additional security measures regime and a lot of those relate to screening and to air side access, primarily. I would prefer not to go into detail as to what the measures are, but they strengthen the screening process and they strengthen air side access and access to restricted areas.

Ms PLIBERSEK—We have heard evidence that suggests that there have not been many changes and that there has been more talk of change than actual change.

Ms Graham—Without knowing what that evidence is, I am not sure that I can answer the question. Can you be more specific?

Ms PLIBERSEK—For example, we have had evidence that suggests that air side security is a major weakness, particularly at Melbourne airport, that contractors and others working air side retain passes for too long, that passes are not handed in at the end of jobs and that passes do not indicate appropriately where air side you can be—you might have permission to be working on a building site but maybe not to be under the belly of a plane somewhere and the pass does not show that. There has been a whole list of suggested weaknesses there in air side security. But you say that no—

Ms Graham—I am very surprised to hear it because, in terms of access cards or aviation security identification cards, we have very strict processes in place. We have training regimes; we have background checks. There are processes in place to ensure that those sorts of things do not happen. I am not saying that there are not individual cases where maybe a card is not filled out with all the bona fides checked. Maybe those things happen, but they are certainly not as a result of processes or systems not being in place. Correct me if I am wrong, but I think you talked about work areas.

Ms PLIBERSEK—Yes.

Ms Graham—Our works areas are quite strictly supervised because we actually have work safety officers there whose job it is just to supervise the sites. There may have been some breaches that have occurred, not that I am aware of them, but the processes are in place to ensure that that does not happen; so I am a bit surprised to hear that. We audit it too.

Ms PLIBERSEK—You audit the return of the cards or what you do?

Ms Graham—Yes, we do. Yes, we audit our cards.

Ms PLIBERSEK—What proportion of ASICs would be returned after someone leaves employment at the airport?

Ms Graham—Are you talking about permanent cards?

Ms PLIBERSEK—Yes.

Ms Graham—We did an assessment of this fairly recently. Between 10 and 15 per cent—around the 12 per cent mark—are not returned. We then take action to try to have them returned, but sometimes people have left their place of address or we have not been able to track them down. But it would be no greater than 10 to 12 per cent.

Ms PLIBERSEK—With people who are signing in to make deliveries air side, what sort of information do you collect on them and how confident are you that that information is enough to at least be able to identify someone who does something wrong?

Ms Graham—We adhere to the general standards and principles that are established by DOTARS. That is through our model ASIC program. There are two kinds of passes that we issue. One is the permanent aviation security identification card, and we go through the process of a criminal background check and so on before we issue that. We also establish what the person's requirement is to be air side and how frequently they need to be air side. The other type of card, probably the one that I think you are more concerned about, is the visitors pass. But to ever be issued a visitors pass the person would always be with somebody who holds a permanent ASIC, someone who is a member of the company or a contractor that wishes to have access to a particular part of air side. Therefore, we would establish the bona fides through that particular supervisor before the visitors pass is issued. Then of course once they go air side they must be under supervision at all times.

Ms PLIBERSEK—They have to have someone with an ASIC with them. Say they are making a Coca-Cola delivery. Do they have to have someone from Coca-Cola Amatil with an ASIC sitting in the car?

Ms Graham—Either they have to have an ASIC holder with them or they are under escort by somebody with an ASIC. We are audited twice a year by DOTARS. This is one of the things that they usually scrutinise quite carefully. It might happen that—and I will give an example—somebody is being escorted to a loading dock to make a delivery to a coffee shop. Very occasionally what has happened is that the escort driver has taken them to the loading dock, the escort driver has been called back because there are a number of escorts waiting and they might have left the person there for a few minutes unsupervised. In fact, we did find that this had happened, so we put in a process where, if the escort driver had to go back to the gate because there were a number of other escorts, they simply took the person back with them and they went back to the end of the queue. So there are processes to try to address those sorts of things, but security is always about human factors. I think we have very good processes and procedures in place, but occasionally people do not always follow them. We are fairly vigilant about doing something about that if we ever discover that is the case. So I would be surprised to find that there was any sort of widespread misuse of the visitors pass or the permanent ASIC system.

Ms PLIBERSEK—I know that you are a little bit unwilling to go into specifics, but I think the nub of what we are talking about is what additional measures you have introduced at the airport for additional security since September 11. One that you have measured is explosive trace detection. I think that came on line in Sydney not so long ago. As an airport user, it is pretty difficult to see how screening and so on has changed.

Ms Graham—There are probably two ways to answer that. The first is that we have implemented all the additional security measures that we have been asked to do by DOTARS. The second is that we have strengthened some of our existing processes so that they are more robust. Perhaps I could give an example of what happens at the screening point. What we do now is regular systems testing. We did not used to do that. The screeners undergo a reasonably good training process before they come on line as a screener. What we actually do now is to have a roster of all our staff that will undertake a systems test to ensure not just that the process is in place but that it is robust.

Ms PLIBERSEK—Do you mean that you hide a weapon in a bag and see if your staff pick it up?

Ms Graham—It could be a weapon in a bag. It could be something in a shoe. We test both the walk-through and the X-ray unit. What I am alluding to there is that we have tried to strengthen some of our existing processes rather than add a new range of processes, other than the ones that we have been actually asked to do. We have also strengthened our access control arrangements in that we have closed off a lot of access points around the airport. So, to a large extent, we have reduced the ability of people to go through different doors and gates. There is more CCTV. So it is more about strengthening what we have there rather than necessarily introducing a whole new range of measures, because we do rely on the department to introduce what we call new procedures in security.

Ms PLIBERSEK—I have one final question. Some of the evidence that we have had—not necessarily about Melbourne airport but about airport security generally—is that, because a lot of the work is contracted out, the work is often undertaken by casuals and part timers. Some people have raised concerns about that, saying that it is quite a specialised job, that it is a high-pressure job, that it is not an easy job. What assurances do you have that the staff that the contractors are employing in airport security are properly trained, that they have reasonable job satisfaction, that they are not being rotated inappropriately to other types of security jobs, that they have specific airport training—basically, that they are appropriate for the work?

Ms Graham—I certainly support your comment that it is not an easy job. I think screeners perform a very important function. It is certainly not as easy as people think it might be. We have a very strong relationship with the contractor. Our security manager is meeting with the contractor daily. So it is not a hands-off approach. We are involved in assessing their training records, making sure that they are complying with all the requirements that are in the manner and occasion of screening documentation. So, if there are any OH&S issues, we have often been involved in assisting with dealing with issues where the screeners feel that they are not being provided with the correct facility. So it is really a daily interaction process.

As for the casual staff issue, Group 4 are our screening contractor, and their policy is to have as few casual staffing as possible. Sometimes you have to have that just to be flexible, but they try to use permanent staff as much as possible. So I do not see that as a really critical issue. The other thing is that, whether staff are casual, permanent or whatever, we insist that they meet the requirements irrespective of whether they are casual or permanent. The appropriate training and training documentation have to be in place. As the client, we do not see any difference between different types of staff. They all have to meet the standards.

Senator WATSON—From your discussions with Mr Barlow of his experience at Heathrow, how does security at Melbourne compare with Heathrow? For example, are there similar risk assessments at both airports?

Ms Graham—The risk assessments would be, I assume, not dissimilar in process from those in Australia. I do not have a detailed knowledge of them.

Senator WATSON—In your discussions with Mr Barlow, has he mentioned any differences between them?

Ms Graham—Yes.

Senator WATSON—What are the main areas of difference in approach between Heathrow and Melbourne? I know his experience there goes back a little while.

Ms Graham—It does. I think there are some more intense search procedures in screening.

Senator WATSON—Here?

Ms Graham—No, in the UK. For example, they do physical bag searches at the screening points.

Senator WATSON—On a random basis or on a selective basis?

Ms Graham—I am not sure, but I know it is part of the process. The other main area is that for some time—and this would go back, I think, to well before September 11—they have had fairly intense staff access control procedures. There is not just screening for passengers but screening for staff as well. Their access control, particularly for staff, is quite rigorously managed. As I understand it, they would be the two key areas.

Senator WATSON—Why do you think you did not implement those measures in Melbourne? Was it a lower risk assessment?

Ms Graham—I am trying to speak for Chris on this. There has been a longstanding threat in UK airports going back 20 or more years.

Senator WATSON—That is right. That is why I asked the question.

Ms Graham—The regulator in the UK, the equivalent of the department here, would, as I understand it, have implemented some of those measures or set them in place based on the threat level and the risk assessment at those airports. At our airport or at Australian airports we take direction from the department on what the threat level is and therefore the associated risk.

Senator WATSON—I accept that. Given Mr Barlow's experience with high security at Heathrow, why would he not have looked very closely—certainly after September 11—at the UK provisions rather than at those of DOTARS? After all, he is managing an airport.

Ms Graham—I understand what you are saying. We did discuss some of those measures, but, as I said, we take our threat assessment and risk management advice from the regulator in Australia, not the UK.

Senator WATSON—But you can see my point. If Mr Barlow has had experience with high-threat assessments—and along comes September 11—I would have thought he would have wanted to perhaps look at standards even higher than DOTARS's to give that added sense of security at an airport that the Australian Pacific Airports Corporation owns.

Ms Graham—Certainly it has been discussed. We did consider and look at some of the measures that might be in the UK—screening, physical searches and so on—but we decided that, because we are in the Australian scene, we have possibly a different threat level and the department is in the best position to be able to determine what that threat level and risk is, because of its access to all the agencies around the world. For example, the department is talking to the UK and US regulators as well. We believe that, because we are an Australian airport, we must take our lead from the regulator in Australia, not in the UK.

Senator WATSON—In other words, you do not have planes flying directly to Israel, as a high-threat assessment?

Ms Graham—No, we do not.

Senator WATSON—What is your view of the demerit approach in the regulations? Can you see any satisfactory alternative to the demerit approach?

Ms Graham—We do not really have a major issue with the concept of a demerit system per se. We just could not understand how it was being put together. There was not a lot of clarity about the actual system that was tabled. The key issue for us was how it would be applied—what would the consistent standards in applying it be. For example, would the regulator issue demerit points at one airport, if they went air side and saw that somebody was not displaying an ASIC, and not do it at another airport? We were very concerned about how it would be applied, what would the training for the department staff be in applying it and, also, who would it be applied against. Would it be applied against the security program holder or would it be applied against the individual who was infringing the system?

An example would be a Qantas employee on our apron not displaying an ASIC. I am not saying a demerit points system would be applied to that but, if it were, would it be applied to us, as the overall airport operator; would it be applied to Qantas, as the program holder, and would it also be applied to the individual? There was no clarity or real explanation of how the system was going to work. We were not so much concerned about the concept of it. In fact, the current regulations do provide for the department to prosecute at the moment, but this has never been applied, as I understand it. The concept was not really the issue, but certainly the application and the structure of the system was. It never got to the point where it really advanced very far. We were told recently that, whilst it is still in the bill, it is not in the regulations; it is being, if you like, put on hold until some further investigation into an appropriate system can take place.

Senator WATSON—So it is not going to be applied then?

Ms Graham—No, not in the short term.

Senator WATSON—What other countries apply this sort of demerit approach?

Ms Graham—I really could not tell you.

Senator WATSON—Could you find out? Is this just an Australian concept or idea?

Ms Graham—I would imagine it is not. It could be that there is a similar type of arrangement to what is in the regulations now, where there is the ability to impose a penalty for noncompliance, but I really could not tell you; I do not know.

Senator WATSON—Some of the unions and others have complained about a lack of training, apart from cabin crew, pilots and those very close to the proximity of the airports. That seems to conflict with what you have said, that you look at the training procedures adopted by your contractors et cetera.

Ms Graham—The contractors are required to meet a certain standard. There is an accredited passenger-screening training standard that was introduced approximately three years ago in partnership with Kangan Batman TAFE. The contractors are obliged to meet that training standard. That involves about three days of training off screening point and then approximately 40 hours supervised training.

Senator WATSON—What about the training of your check-in staff?

Ms Graham—I am not responsible for check-in staff.

Senator WATSON—That is a Qantas responsibility, is it?

Ms Graham—That is the airlines' responsibility.

Senator WATSON—So you do not have meetings with them about the training that takes place?

Ms Graham—We have regular meetings with the airlines about aviation security matters, but we have not discussed check-in staff because we see that very much as an airline responsibility.

Senator WATSON—But, in a sense, don't you think you have a responsibility to liaise with them to make sure that they have a high degree of training for anything that comes onto your property? I feel it really must go beyond just securing screens, sensors and that sort of thing.

Ms Graham—I totally agree. For our security committee, any of those sorts of issues can be raised, and we are interested in how all our tenants or airport users are complying with regulations. Check-in is perhaps an example of where we have not had anything raised in terms of security. It has not been a focal point for us because it is primarily a passenger facilitation issue more than a security issue or because we have not had any security issue about it raised.

Senator WATSON—Do you have representatives sitting in on your contractors' training programs, or do you just take for granted what they tell you?

Ms Graham—We have not had anyone sitting in on a training course, as far as I am aware, but we certainly audit their training records to ensure that the training is being carried out.

Senator WATSON—So you look at the paperwork without—

Ms Graham—We look at the paperwork.

Senator WATSON—looking at the actuality.

Ms Graham—Yes. I would like to take that on notice because there may have been somebody sitting in on a course that I am not aware of.

Senator WATSON—But as a practice you do not sit in on all their courses?

Ms Graham—No.

Senator WATSON—I do not necessarily mean every one.

Ms GRIERSON—If you have some concerns about a demerit system, how do you think compliance is best brought about?

Ms Graham—The department has never implemented a compliance system with us. As there are regular audits and regular meetings with the department, I just do not see that a formal compliance system is absolutely essential.

Ms GRIERSON—So when was the last time DOTARS did a random audit at your airport?

Ms Graham—A few months ago.

Ms GRIERSON—Was it random or were you notified that they would be there?

Ms Graham—We were notified that they would be there.

Ms GRIERSON—Have they ever done a random check?

Ms Graham—If the department are out at the airport, they are walking around and they observe something, yes, they can certainly undertake a random check. They certainly do in terms of screening. They will bring anything to our attention if they happen to be out at the airport and they observe something to be not correct.

Ms GRIERSON—We have received evidence that suggests that the 'she'll be right' culture and a risk management culture are having some difficulties enmeshing at the moment and that there is some complacency regarding regular contractors visiting—that regular deliveries et

cetera are a regular occurrence and therefore do not need constant checking. Are you aware of that?

Ms Graham—As I said before, I am certainly not aware of any particular issues that have occurred recently in that area, but I probably should make the point that we are accountable for an airport that has roughly 10,000 employees. Obviously there are myriad types of tenants, users, contractors and there are varying degrees of acceptance of security being really important. One of our biggest focuses in the last year or so has been to try to build that security culture, because security is always about people and human factors. We cannot do all the security ourselves, so we have to build a strong culture. I think we have been quite successful in that, but there will always be perhaps some companies that are very focused on doing a particular job that just are not quite so security aware.

Ms GRIERSON—Do you have any concern that, when you devolve security to a contractor, you perhaps also give away that sort of responsibility?

Ms Graham—With the screening contractor, no. We have so much of a constant, daily relationship with the security contractor that that is not really a concern for us at all.

Ms GRIERSON—How often do you have airport user meetings, say, of all your tenants and users of the airport?

Ms Graham—We have a security committee that meets every two months. There is not a representative of every single organisation, but broadly the major players are represented at those meetings. Attendance can be anything from 15 to 25 people.

Ms GRIERSON—Do you have an overall airport security plan in place?

Ms Graham—Yes, we have an airport security program, which we are actually required to produce under the department's standards. It is actually approved by the department.

Ms GRIERSON—Do you think the different responsibilities and roles of all those layers that operate within an airport are well defined and understood?

Ms Graham—We do our best to ensure that they are. Again, there are probably two key points about security. On the one hand, you have screening and searching people and, on the other, you have an ID system that has the appropriate checks behind it. Those are the two key elements of protecting your security. We try to do as much training as we can of every single person who applies for an ASIC. When you apply for an identification card, you have to go through an induction training course before you get that ASIC issued. Other than that, we do not do a lot of ongoing security training—we are not really resourced to be able to do that—but we do try, through signage and newsletters, and obviously through our patrols, to keep that security culture going. We have people patrolling air side and the terminal just as a visible presence.

Ms GRIERSON—Would you know what percentage of your annual budget you are spending at the moment on security?

Ms Graham—I am going to hazard a bit of a guess here, but I am fairly certain I am in the ball park. Between 15 and 20 per cent of our budget would be spent on security.

Ms GRIERSON—Do you think that is excessive?

Ms Graham—No, and I have to make the point that a lot of that is actually recharged back to the industry.

Ms GRIERSON—Does that mean passengers too? I suppose it does really.

Ms Graham—Yes, back to the passenger.

Ms GRIERSON—In your submission you say:

The overall coordination of security at a airport is best carried out by the operator. The relationship between airlines and tenants in the corporate sector and other stakeholders is sound. However, when Federal bodies are involved such as the AFP in this coordination role it is often disregarded by them.

Do you mean the AFP disregard those relationships? I could not quite understand what you meant. You went on to say:

This needs improvement.

Ms Graham—I am probably talking more about the Australian Protective Service, which is now a division of the AFP. Previously it was part of the Attorney-General's Department.

Ms GRIERSON—Why is it making it more difficult—too many people to deal with?

Ms Graham—From our point of view, probably the fact that the APS—and there are obviously reasons for this—like to act fairly autonomously. I can understand there are jurisdictional reasons for that occurring, but it can make it difficult for us, as the overall airport operator, because the APS are obviously very much our surveillance, patrol, counter-terrorist organisation and we need to have a close partnership approach with them. There is an interesting conundrum, I suppose, in that the Australian Protective Service are like a service provider to us as a contractor, but obviously the AFP would see that they need to maintain their independence and that just creates a bit of an issue for is in terms of communication and coordination.

Ms GRIERSON—Have you used Launceston airport to trial more rigorous security measures?

Ms Graham—I am sorry, I am not really able to speak for Launceston. I did mean to say that at the beginning of the hearing.

Ms GRIERSON—You mentioned some bomb detection strategies being put in place. Were they trialled at Melbourne or do they happen?

Ms Graham—Yes, they do happen—at the passenger screening point.

Ms GRIERSON—Do you test for substances?

Ms Graham—Yes. It is a wanding system that looks for traces of different types of explosives.

Ms GRIERSON—Have you introduced, as some airports have, the measure of putting forward your photo ID and your boarding pass at point of screening for entry into departure lounges?

Ms Graham—I am not aware that any airport has done that. We certainly have not done that. I am just not sure what sort of security outcome that would generate.

Ms GRIERSON—It takes a long time.

Ms Graham—Yes, it would take a long time.

Ms GRIERSON—Thank you very much.

Ms KING—What sort of penalties apply under the contract that you have with Group 4 if you do not believe they are training their staff to the level that is required?

Ms Graham—Under the contract, we do have a KPI system, and it is a financial penalty system that we can invoke if the contractor is not meeting certain things—and obviously that means that they are not complying with the standards in any way.

Ms KING—What sort of things would the KPIs cover?

Ms Graham—Compliance with regulations is the principal one—any sort of breach—failure to meet a standard during an audit and some reporting to us on particular things would be the three key areas.

Ms KING—Would you monitor things like their turnover?

Ms Graham—We do not monitor it. It is a contractor relationship: we do not directly manage, so we expect the contractor to manage certain elements. We would expect them to manage staff turnover and things in that HR type area as long as anything they do in that area does not impact on their performance. Obviously, if we become aware that there are some sorts of IR issues occurring, we then get involved. But, as a general principle, we try to maintain a bit of a hands-off approach to some of those areas and let the contractor do what they are paid to do.

Ms KING—How long is your current contract with Group 4?

Ms Graham—It has another two years to run with a two-year option at the end.

Ms KING—Thank you.

Ms GRIERSON—You made the comment that at Launceston there is no Commonwealth security presence—no Federal Police, APS et cetera—and that that is common in most regional airports. Do you have a view on that?

Ms Graham—I really do not want to speak about Launceston. I have very little to do with it, and I would probably be doing them a disservice.

Ms GRIERSON—Thank you.

CHAIRMAN—The submission of the Australian Airports Association criticised the department for a lack of consultation with them during the development of the draft aviation security transport regulations. You emphasised the importance of consultation. Did you have any problem with the level of consultation during the drafting of those regulations?

Ms Graham—I think the department did their best to consult appropriately on it. I think there were deadlines imposed on them that meant they were trying to move it through very fast. At some of the consultation forums the documentation that was tabled was not really enough for us to make good judgments about what was being proposed. In other words, rather than seeing the regulations, we were seeing some papers about the regulations which did not necessarily give us the clarity that was needed. A couple of times we thought we were going to see things before they went into parliament and we did not get the chance to see the final documents. I think they have genuinely tried to consult and they have provided those forums for consultation. The department really makes quite a strong effort to consult as widely as they can. I just suspect that at times they are under time constraints, and perhaps some resource constraints as well, that make it not as effective as it could be. If I was to compare it to some other agencies, I would say their consultation processes are fairly good.

CHAIR—The Auditor-General's report was not critical of DOTARS's response to aviation security issues raised by September 11—in fact, as I recall, it was probably complimentary—but it was very critical of their lack of formal paperwork surrounding risk analysis and associated issues of mitigating risk in a formal paperwork sense rather than taking care of it on the ground. The department responded to that by saying that they had been too busy trying to keep passengers and airlines safe. Do you have a response to that or did that follow the same line that you just took when it came to consultation on the regulations?

Ms Graham—I do not know about the department's documentation at the Canberra level, but in our audits we always get the appropriate follow-up paperwork. They are obviously under some pressures in getting papers and minutes out—those sorts of areas—but I cannot comment on why. I think the point has to be made, though, that as part of the consultation process the department and the industry have implemented working groups over the last year. Those working groups include industry, government and the major players and they look at particular areas of security—it might be screening or ID cards—and those have been very successful forums for developing policy. Again, I think that adds to the workload of the department in terms of paperwork, records of meetings and so on.

CHAIRMAN—In your submission you stated that regional airports needed more power over their tenants to ensure compliance with security programs. Bankstown airport made the same

point, giving an example of a tenant who could not be compelled to close their air side access gate. What powers do you currently have to mandate security at Melbourne?

Ms Graham—Very little. From our point of view, it is one of the areas where we would like to see stronger enforcement provisions in the new regulations that would enable us to get other users of the airport, or operator tenants, to comply with security requirements. It is quite a battle at times. We have to use consultation arrangements to encourage people to comply rather than being able to use much in the way of enforcement powers with teeth.

CHAIRMAN—Is it appropriate that that be in the federal regulations or is that a state government responsibility?

Ms Graham—I would have thought that at the airport level it would have been a federal responsibility. I have not really thought about that.

CHAIRMAN—So you would be happier if the Commonwealth improved your powers to regulate users that could perhaps compromise the overall security at Melbourne airport

Ms Graham—Yes, very much so. At the moment, for example, one of the issues we have air side is the display of ID cards. From a security point of view, there are merits about the display of ASICs, but often the person has got an ASIC and they are simply not displaying it because they might have a safety vest covering it. That is still seen as a breach of security. Obviously, in trying to encourage people to be very vigilant about that, you need either to continually promote the culture—it is an education program and so on—or, as we do at Melbourne, to suspend the ASIC for a period of time, or we might look at suspending access control for a short period of time. But really we do that off our own bat. There is no provision for us to do it.

CHAIRMAN—We understand—that is, we have been advised—that Australia's major airports are regularly audited by overseas countries whose aircraft fly in and out of our jurisdictions to see whether we come up to scratch. We are told that they continue to give us a AAA rating, if that makes sense—a five-star hotel category. I would like to know whether you pay for external audits of your control of air side operations, which probably does not fall within that international examination.

Ms Graham—Last year we did have the British Airport Authority do a peer review of the airport. That included safety, not just security; it was air side safety and also security and fire safety in the terminal.

CHAIRMAN—Could you make that available to the committee?

Ms Graham—I am sure we could.

CHAIRMAN—Would you?

Ms Graham—Yes, I am quite happy to do that.

Senator WATSON—Do you have a high-security fence on the eastern boundary of Launceston airport.

Ms Graham—Again, I cannot comment. If I could comment, I would. I just have not been to Launceston recently to be able to comment on it.

CHAIRMAN—If we have any further questions, do you mind if we put them to you in writing rather than make you come back again?

Ms Graham—No.

CHAIRMAN—Your boss is certainly welcome to appear at a future hearing, and he can make those arrangements with Dr Carter. Thank you very much.

Ms Graham—Thank you.

[10.45 a.m.]

EDWARDS, Mr Bevan George, Secretary, New South Wales Division, Regional Airports Representative, Australian Airports Association

PIPER, Mr David Rodney, Deputy National Chairman, Australian Airports Association

VALLENCE, Mr George Joseph, Member, Australian Airports Association

CHAIRMAN—Thank you very much for coming and thank you for your submission. Do you have a very brief opening statement?

Mr Piper—A very brief one, yes. The Australian Airports Association is here representing its 255-odd members. We wish to make an informative positive contribution to your debate. I would have to say that we are conscious of the necessity and the cost implications, particularly of the physical compliance. In that respect, I have with me today George Vallence, who is the airport manager at Mildura, a category 5 airport, and Bevan Edwards, who is airport manager at Coffs Harbour.

CHAIRMAN—We have met Mr Edwards.

Mr Piper—That is all I have to say. I will leave it to my colleagues to present their submission.

CHAIRMAN—Thanks for that. In a few minutes I am going to turn into a pumpkin. It is not because I do not like you or do not think that what you have to say is important, but I am not well so I am going home. I have plenty of colleagues and I am informed that the Labor ladies are likely to take over the hearing.

You were fairly critical in your submission of DOTARS for not consulting, yet the last witness we had from Melbourne airport and the Australia Pacific Airports Corporation thought that consultation was probably pretty good—that, while it could always be better considering time constraints, consultation was not bad—and that cooperation of the industry with the department has been very positive. Is it the fact that you as an organisation were not being consulted or that consultation was just very poor in general?

Mr Piper—I am not entirely sure you have interpreted that correctly. I will ask Bevan Edwards to run that for you.

Mr Edwards—I am not too sure which part of the submission you drew that information from. Generally, the association feels the department regulates aviation security in a satisfactory manner and the department does its best to accommodate the demands put upon it by industry and by government, depending on resources of course, and the experience of most of the members is that we have very good cooperation with DOTARS at an operational level. I can only assume that the association is concerned more about the consultation during the initial

stages of the new security measures that were brought in after September 11. In that respect, it might just be the hastiness and the speed with which those were introduced.

CHAIRMAN—It was submission 5, page 2, where you stated that 'the views of aviation industry experts were' in many cases 'totally ignored' during the consulting process. That is pretty straightforward, I would have thought.

Mr Edwards—Point taken. I cannot add comment to that, I am sorry.

CHAIRMAN—So you are not that unhappy with the degree of consultation?

Mr Edwards—No. I can only reiterate what I said before. I think it was the speed at which the new requirements were brought in after September 11 that was the issue that the association was raising.

CHAIRMAN—You have a cooperative relationship with DOTARS?

Mr Edwards—Certainly on an operational level.

CHAIRMAN—The demerit system that is proposed in the regulations has received some criticism for lack of detail and perhaps supposed ineffectiveness. Could you give us comments on what you think of the proposed demerit system?

Mr Piper—The answer is no, I cannot. I have not come to grips with the demerit system as such.

CHAIRMAN—Let me ask you the question in a different manner. The audit report, which led to our inquiry, was—and correct me if I am wrong—critical of Qantas. I think it was Qantas, but perhaps it was others as well. An error was made at a screening point and the audit report felt that appropriate discipline was not necessarily taken. Do you think it is important that there are sanctions and penalties on sloppy work when you are talking about a critical issue like screening?

Mr Edwards—I am happy to comment on that, coming from an airport where we do have screening. I think the demerit system is a good system, provided that it is implemented correctly and in such a way that it is effective. When you are dealing with people, you have different levels of security and different ways that people approach their work. It is like any workplace where you have to deal with different sorts of employees. But there needs to be some recourse for people that are not performing well. I think employers need a backup in that respect to appease the unions and the like. I think a similar system has been proposed by CASA for its regulatory regime as well, and I think that is a good way to go. It seems to be successful with motor vehicle licences. Generally, we support that.

CHAIRMAN—Are you satisfied in general that the audit mechanisms that we have in place for checking compliance with screening regulation No 1 at various airports and the ability of the screeners to detect unlawful items in hand luggage is satisfactory?

Mr Edwards—Again, I will comment on that. My two colleagues are not involved with passenger screening at airports. The art of screening is a moving feast—you have to keep one step ahead of the opposition. I think with the technology we have at the moment our screening is the best it can be. Again, human nature comes into it and it is a matter of making sure that people do not spend too much time in front of a screen and that they are rotated. Certainly, from my observations, the auditing that takes place by the Department of Transport and Regional Services is adequate. We are not the screening authority at my airport, Qantas is, but I believe there are also internal audits. I think it is one of those areas that we need to review regularly because people do become complacent as time goes on, particularly in an environment where you are not detecting too much—and a lot of regional airports would be like that. You need that buzz every so often to keep you on your toes.

Ms GRIERSON—I am interested in regional airports in particular and how they interact with the Australian Federal Police and their local state police, which are often not immediately accessible or available. Do you have any experiences or comments on whether regional airports do feel supported in that way or would request more presence of, say, the Australian Federal Police?

Mr Edwards—You are talking about a very big nation and a wide variety of situations. I think in the larger regional centres the support is very good. Certainly, from my own experience, we can contact senior police officers within our local area command at very short notice, and we work with them in other areas as well as security, such as emergency response and the like. Obviously, in the more remote areas, it becomes a problem. I know there are cases of individual airports that, for whatever reason, do sometimes have concerns with the response they get at things like emergency meetings and the like. As far as the Australian Federal Police goes, obviously it is a little bit more difficult to make contact with a lot of the Federal Police.

Ms GRIERSON—So you would not have any presence of AFP in Coffs Harbour?

Mr Edwards—We are one of the lucky ones; we do. They work closely with us in conjunction with Customs, AQIS and the local police. But we are a fairly large centre.

Ms GRIERSON—You are a very large centre. You mentioned the cost to regional aviation and some concerns about who should pay for that. I think Horizon, which fly into Coffs Harbour I think—

Mr Edwards—Grafton and Taree.

Ms GRIERSON—They have just gone into voluntary administration. Do you think the costs are perhaps burdensome? Do you think governments should be making some specific contribution to security at regional airports?

Mr Edwards—The short answer is yes, we think there should be some assistance.

Ms GRIERSON—What form could that take?

Mr Edwards—It really depends on the airport and the situation and the level of security that will ultimately be introduced. I think the important thing here is that, as part of this process,

there should be risk assessments done on each individual airport to determine the level of security that is needed. But, if you take it to its extreme, even if an airport like Coffs Harbour—where we have a fairly large passenger turnover—were to have, for example, checked-in luggage screening, you could be looking at something like $600,000 to $1 million just to implement that.

Ms GRIERSON—So do you think equipment would be a major cost or would it be staff levels that cost more?

Mr Edwards—Obviously, initially the equipment and any building alterations that went with that. Ongoing costs for manning those points, depending on the throughput of passengers, could be in the order of $2 a passenger.

Ms GRIERSON—But it is hard to pass on the major technology changes that are happening?

Mr Edwards—Yes, and the problem with that is that some of that technology only has a life of five years or less, so you are always upgrading it.

Ms GRIERSON—You make some comments about the Commonwealth government playing more of a leadership role in assessing emerging technologies and making recommendations about that. Does that happen at the moment or is it really left to the industry?

Mr Edwards—It is really left to the industry. I suppose with regional airports we are that little bit more removed, so we are not au fait with some of the changes in technology that the capital city airports are exposed to.

Ms GRIERSON—Is servicing and maintenance of this sort of equipment ever a significant problem in regional airports?

Mr Edwards—It is certainly more costly than in a capital city, because you have to bring people up from the capital city and you need to accommodate them generally. So, from my own experience, the annual maintenance contracts for a particular piece of equipment could be 50 per cent greater than in a capital city.

Ms GRIERSON—That is burdensome. You also make some interesting points about NAS, the National Airspace System. You claim:

> ... we find it inconceivable that any Government could allow any aircraft on the Australian register into the sky without i) a radio for communication purposes, and ii) a mandatory requirement to use the radio when in the vicinity of an airport.

Do you have concerns that that is the case and that such civil aviation practices and small planes pose a risk?

Mr Edwards—The association is concerned that there are operators or pilots that can go into some airports, particularly the busy airports, without making calls. The association believes that that means there is a risk they might sneak in unannounced and maybe do something or be somewhere they should not.

Mr Vallence—One other concern we have in Mildura is that, with ground maintenance and runway maintenance, we now have the ground staff call on an MBZ frequency and alert pilots and also get acknowledgement of that when they are actually performing duties on the runway. They still have an avenue to make an announcement, but there will not be any mandatory response, and that is a concern from a safety point of view.

Ms GRIERSON—Have you formally taken that up with DOTARS or CASA?

Mr Vallence—Yes, it has been broached with DOTARS.

Ms GRIERSON—They will probably not be doing it over Canberra on Thursday!

Mr Piper—We have had meetings and correspondence directly with the minister.

Ms GRIERSON—Good. Do you have a response?

Mr Piper—Our concern is fairly well expressed, but we are not entirely sure of the interface of new technology, and that has not been well explained by either of the departments concerned. But we are aware, for instance, of the minister's recent announcement regarding the virtual radar which is to be established through the construction of 20 ground stations using satellite information from aircraft transponders. My guess is that 90 to 95 per cent of aircraft in Australia are fitted with transponders; we merely need that technology to catch up with us and for it to be explained to us and our membership. It probably means that, with an interrogator station on the ground, we can identify most aircraft coming over our airports. But we do not quite know what the technology is, and that maybe the gap that will cover our concerns about the mass implementation.

Ms GRIERSON—I think the Australian public would assume that you could identify every aircraft at all times over all Australian airspace. That is obviously a goal that will be realised one day. Will those costs be passed on too?

Mr Piper—The transponders are in most aircraft now. The linkage will need to be with their GPS systems, to download their coordinates, and an interrogator system on the ground. Frankly, I have no idea what the costs would be. It would currently cost about $20,000 to merely establish the survey points and procedures for a new GPS approach to an airport, so I guess it would be somewhere between that figure and $100,000. But that is an absolutely wild guess, because we do not know what the technology is going to come down to.

Ms GRIERSON—Uncertainty is never a good thing in business, is it?

Mr Piper—It always leads to conjecture.

Ms KING—In your submission, you are fairly critical that politicians and some bureaucrats are not really aware of what the costs of upgrading security at regional airports would be. What exactly do you think the costs would be?

Mr Vallence—I can probably talk from Mildura's point of view.

Ms KING—What would be required to improve security at Mildura airport?

Mr Vallence—We estimate the cost of the security equipment to be in the vicinity of $600,000. That would be $100,000 a year, paid back over five years. So the cost of the equipment would be about $500,000.

Ms KING—Are you talking about baggage-screening equipment?

Mr Vallence—Yes, just baggage screening—without checked baggage.

Ms KING—Is there currently no baggage-screening at Mildura airport?

Mr Vallence—No, there is not. That is confusing for passengers, because they get on board and travel to Melbourne and then they are security checked on arrival. So it is a community issue. We think the recurrent cost would be in the vicinity of $330,000 to $400,000 per annum. Adding those two factors together, we think it would contribute to about $9 extra per passenger ticket. So we are back to having another levy.

Ms KING—I have not been to Mildura airport for a long time. What size plans are you flying in and out of there at the moment?

Mr Vallence—We fly Dash 8s and Saab aeroplanes, which are 36 to 38 seaters.

Ms KING—There was a comment before, in terms of screening staff, that some of the conditions of employment—such as sitting at a screen for too long—can impact on whether people are able to do a good job. The union commented that some of the conditions of employment around remuneration and the morale of your security staff can have a fairly large impact on people's performance as well. Would you care to comment on that?

Mr Edwards—The comments I make are on regional airports; I cannot make comments about capital city airports. At regional airports, you tend to have local contractors. In regional Australia, if you have a job you are usually happy that you do. From my own experience, the airport does not employ local contractors, because they are employed through another contractor that is ultimately contracted by Qantas. Generally, when the local contractors come to me and have a bit of a whinge session, it is not usually about pay and conditions; it is usually about rosters and those sorts of things. Having said that, I understand the job could be very difficult with periods of concentration and that sort of thing. There would be a need for staff management. I cannot comment on pay because I have no idea what the screeners are paid. It should also be remembered that at regional airports there are quiet periods between flights, whereas at larger airports they are working flat out all the time.

Mr Piper—We have taken the view that we would be talking about regional airports simply because the major airports are likely to be attending directly on their own behalf—and the witness prior to us was one of those. They are members of the association, but we will leave them to make their own submissions.

Ms KING—I want to go back to some of the issues about cost. Certainly, we have heard quite a lot of evidence about who will bear the costs if there is a need to upgrade security at those

regional airports. From a parliamentary point of view, before September 11 we would never have imagined that an aircraft would be used as a weapon—somehow we did not comprehend that that was going to happen. Given that regional airports do not on the whole have a great deal of some of the security things, such as baggage screening, is there a heightened risk from regional airports or shouldn't we be too worried about them?

Mr Vallence—The biggest risk would be if regional airports were used as a feeder to get terrorists to the major airports. Indeed, I believe the September 11 issue was exactly that—they were transiting and they held a flight to get them on, which was a bit unfortunate. That sort of circumstance would be the only circumstance because of the size of the aeroplane needed to damage a building.

Mr Edwards—At the other extreme, if the requirement at a particular airport was to put in a very high level of security, it could really make that airport non-viable. If you are talking about an airport with 30,000 passengers a year, it could be the difference between that airport functioning at a profit or, in some cases, putting it further into the red than it already is.

Ms KING—Are there things that are not that expensive in relation to passenger identification that may increase security in the area you just mentioned where potential terrorists are transiting through a regional airport to get to a major metropolitan one?

Mr Vallence—It is very hard to answer that. You just do not know in today's world who is likely and who is not likely.

Ms GRIERSON—I am from Newcastle and, even though we do have screening equipment et cetera, every passenger is also required to show photo ID and our boarding pass before going into the departure area. Obviously, that is just a manual process and does not require any technology.

Mr Piper—Unfortunately, the matter of cost is like a piece of string. It depends very greatly on the particular airport and the physical infrastructure that is already there. In terms of costs, in some areas they would have to actually rebuild the terminal, not just install equipment. Most of those regional airports are funded by local governments. Whilst security is extremely important, particularly for the national big picture, in a municipality the airport has to take its priority standing from all of the other infrastructure. The rate of income is generally not sufficient to cover major alterations. For instance, whilst it is not a municipal airport, Nhulunbuy—one of our members in the Northern Territory—has to rebuild the terminal completely in order to comply.

Ms GRIERSON—To have a separate area.

Mr Piper—I think it is costing $2 million. If you try to impose that on somewhere like Dubbo, there would be extreme difficulties.

Senator WATSON—The *Australian*'s aviation writer, Steve Creedy, says:

> The union also will tell a federal parliamentary committee ... today that customer service staff strongly support the need to check passenger photo identification at the gate before boarding all flights.

This happens at some airports, but it is not universal. How do you as an association view that requirement?

Mr Piper—I guess we are really waiting to see how the departments impose their stages of categorisation on airports. It would be one of those items that we would have to assess and cost on an individual basis. There would then be the problem of cost recovery. It is obviously achievable, but the cost problem is something that we cannot put a finger on.

Senator WATSON—That leads to the next question. Are you as an association happy with the risk assessment process and outcomes for regional airports and the categorisation that has been agreed to?

Mr Vallence—As far as Mildura is concerned, we are content with the way it is at the moment because I think there is sufficient vigilance there from the staff and from the way we operate in Mildura. I think it is reasonable and I think it is adequate.

Senator WATSON—Mr Piper, what about your other smaller regional members? Are they happy about the risk assessment adopted by the department and the categorisation that has been adopted?

Mr Piper—The categorisation has not gone down past category 5, and I am not aware of any responses from those smaller regionals.

Senator WATSON—Are you happy with the categorisation up to category 5, because there are a lot in categories 4 and 5?

Mr Piper—It appears to be reasonably logical and, in that case, you would be happy with it.

Senator WATSON—You have been fairly critical in some of the statements that you have made. You say:

We also understand that from time to time the 'political process' as such, may impose upon the Department certain constraints that do not necessarily receive the wholehearted approval and support of the industry.

What do you mean by that? It is pretty strong language.

Mr Piper—I suppose you would have to say that, in terms of the number of departments who have shown an interest in security and the diversity of our membership, there is a certain amount of territorial interest and differences and, therefore, the priorities come up a bit differently. That is a non-answer to a question. I could almost be described as a politician in training!

Senator WATSON—Can you put some flesh on those bones for me by giving some regional examples?

Mr Piper—I will defer to my colleagues.

Senator WATSON—How do we know that you have not just picked the best of the regionals to come to appear before us today? That is why I am asking you the question, as one who

represents the broad spectrum. You have two people who have come here today and who obviously have pretty good systems and processes in place. I have asked you a question about all your other clients and you have given me a political answer that is a non-answer.

Mr Edwards—If I may, I will respond. We hold state meetings in which we interact with our membership and discuss these matters, and I believe I have a feel for the New South Wales state members. As for that particular comment that was in our submission, it is my belief that it really arose out of things that happened after September 11. A lot of things happened over a very short period of time and I think the industry thought that there was a lot of things imposed downwards without consultation. Really, that went down only to the categorised airports. Some that had been previously categorised and were not were reinstated. But it certainly did not filter down to the smaller regional airports and the rural airports. Very little has changed there since September 11.

Senator WATSON—Do you stand by your statement? It is a pretty strong statement.

Mr Edwards—I think that really refers to what happened after September 11 and it really refers to those categorised airports and the fact that they had to do things fairly quickly.

Senator WATSON—But you do not say that. Perhaps if you said that resulting from September 11 there was a bit of a knee-jerk reaction, but you say 'from time to time' so there would obviously be a series of problems that you have encountered when you condemn the political process as such. So do you stand by your statement?

Mr Edwards—As far as regional ports go, no.

Senator WATSON—You don't?

Mr Edwards—The categorised regional airports have a great deal of consultation with DOTARS. We can pick up a phone and talk to representatives from DOTARS at any time. Certainly, there has not been a great deal of imposition placed on us over that time, so I think that refers mainly to the larger airports.

Senator WATSON—Mr Piper, you can answer for the larger airports: is that statement 'from time to time' true? You wrote the submission.

Mr Piper—No, I did not.

Senator WATSON—You have to stand by your submission; you obviously approved of the submission.

Mr Piper—On the basis of the information that our CEO had, I would stand by the submission he has made.

Senator WATSON—The statement 'from time to time'?

Mr Piper—Yes, 'from time to time'. He has wider contact with our members than I do.

Senator WATSON—But you cannot tell me what he means by that—apart from September 11?

Mr Piper—No.

Senator WATSON—Would you take it on notice and ask him what he means by it?

Mr Piper—We will get an explanation and respond.

Senator WATSON—Thank you very much. We have another strong statement:

At this time of heightened 'security awareness' we find it inconceivable that any Government would allow any aircraft on the Australian register into the sky without i) a radio for communication purposes, and ii) a mandatory requirement to use the radio when in the vicinity of an airport.

What was the basis for that statement? My coming from Tasmania, some of our people have expressed concerns about the new system. Your statement further raises that sort of concern.

Mr Piper—Indeed, and I think we have partly answered that in response to questions from Ms Grierson and Ms King, and that is that we are concerned that under the new system there will not be a mandatory requirement to make radio calls on approaching an airfield. We consider that would be a breach of safety and security requirements. For instance, in the case of Mildura it would mean that maintenance staff on the runway may well not know that an aircraft was joining the circuit and approaching for a land while they were on the runway.

Senator WATSON—So, under the current regulations, are they required to make contact with the airport or with other aircraft?

Mr Piper—They certainly are in terms of a MBZ, a mandatory broadcast zone, which includes most of the larger regional airports with RPT services.

Senator WATSON—Why do you think they dispensed with that need to have radio communication either with the airport or with other planes in the area to inform them that they are about to land or take off?

Mr Piper—I am sorry, I did not quite catch the first part of your question.

Senator WATSON—You have said that it is no longer necessary under the new rules to have radio communication with the tower, with the ground or with other aircraft in the area. What are the current arrangements that these arrangements have superseded?

Mr Piper—The current arrangements are that an aircraft approaching a MBZ is mandatorily required to make broadcast calls to announce their intended arrival and to indicate the time they will be in the circuit.

Senator WATSON—Why do you think they changed that? That seems a fairly sensible approach to me.

Mr Piper—I do not know why they have changed that. We understand it is the current American system, but we have not received a satisfactory explanation for the change or, indeed, what is likely to happen in the new circumstances—and it does give us cause for concern.

Senator WATSON—And rightly so. Thank you.

Ms GRIERSON—Is airport screening equipment generally leased or purchased by regional airports, in particular?

Mr Edwards—I am sorry, I cannot answer that. From my own experience, we purchased equipment we had before. The current screening authority at our airport is Qantas. I do not know what arrangements they have made. So, no, I do not have that information. We can certainly take that on notice.

Ms GRIERSON—I would be very interested to know, because if there were going to be assistance it may come in one major leasing arrangement or some sorts of benefits.

Mr Vallence—I think the assistance should not only be the hardware, though; it should also be for infrastructure changes to the buildings.

Ms GRIERSON—Yes, that is significant.

ACTING CHAIR (Ms Plibersek)—I thank the representatives of the Australian Airports Association for appearing before us today.

[11.29 a.m.]

LIPMAN, Mr Rob, Australian Services Union Member at Qantas Airways Ltd, Melbourne

WHITE, Ms Linda, Assistant National Secretary, Australian Services Union

STANLEY, Mr Noel, Australian Services Union Occupational Health and Safety Delegate at Qantas Airways Ltd, Melbourne

ACTING CHAIR—Welcome. We have received a submission from your union. Do you wish to present any additional material or make a brief opening statement to the committee?

Ms White—I do. We have made a number of submissions, including two confidential submissions. We filed one with you on 17 October and another yesterday—the statement from Mr Stanley. We also have a written submission, which we filed on the record yesterday. I apologise for their lateness. In the written submission, we alluded to a survey that ASU was conducting, independently of our submission. For the benefit of the committee, I have brought the preliminary survey results for you to examine. The lateness of the results is because the survey is still ongoing, but we felt that it would be useful for the committee to see them. I would ask that that be tabled as evidence from the Australian Services Union.

ACTING CHAIR—Thank you. We noticed the results of your survey in the *Australian* today.

Ms White—As they are not detailed in my submission, it might be helpful if I take you through some of the survey. At the back of the document headed *Preliminary survey results: October 20, 2003* is a copy of the questionnaire that we circulated to our members; it is the original version. In September it was circulated to airports all around the country, and results are still coming back. This report does not include all the answers to the survey. We extracted those that we thought would be of particular interest to you. Basically it is about what customer service staff think, and how they have experienced air rage at their airports.

The survey covered 14 airports, and employees or ground handlers from 10 airlines responded. The airports were of varying size—from small regional airports like Mount Isa, Gove and Ayers Rock to larger airports like Sydney, Melbourne, Adelaide and Perth. The results are basically a collation of the responses of the customer service staff. In our view, they suggest fairly frightening statistics: 96 per cent of respondents had experienced air rage while working at the airport. When we asked them about its frequency, a third of those respondents said that it was almost every day, 35 per cent said once a week and 27 per cent said once a month. We asked them about the sorts of behaviours they experienced. Obviously, air rage, as we define it, covers a range of behaviours. Air rage on the ground is disruptive passenger behaviour. It can be a failure to observe safety instructions, verbal harassment or physical assault. We asked them to detail that.

Obviously the most common behaviours are anger and verbal abuse, followed by passengers being out of control and threatening agents. Seven out of 10 agents said that they had seen a passenger being threatened by another passenger; 32 per cent had seen somebody assaulted, and

there have been incidents of stalking. We then went through what their views were. We asked them if they had been physically touched or assaulted. We have extracted all of those results under five groupings, which will give you a pretty interesting cross-section. It ranges from being chested by a passenger, having briefcases or passports thrown at you, grabbing of arms, following you to the toilet to get your ASIC—an identification which people often wear around their neck—being spat at and being punched. There is a range of things which I detailed verbatim from those surveys.

We also asked them what they thought could be done to improve airport security. Interestingly, we asked them whether they thought security arrangements were adequate. We talked about the APS, the Federal Police and who was there. Sixty per cent of them said they did not believe that security arrangements at the airports were adequate. Where they had to write an answer—which you will see from the survey—177 of them gave detailed responses and wrote down what they thought could be done at their airports. The responses will need significant analysis by us. There will be some differences between airports but there are a range of things that are common between them—certainly about having better and quicker response by security people, having APS do their job, having passengers not in check-in areas and having passengers not in security areas. I think somebody suggested—it may not be a strategy—that pepper spray be issued. That is an extreme example but it was probably from a person who was subject to an extreme incident. There is a range of fairly helpful suggestions about how things could be improved and what they believe would make their workplace a safer place for them.

We asked them about the incidence of prosecutions of offenders, which was very low. One per cent said the offender had been prosecuted. We asked them whether they thought penalties should be tougher and they thought they should be. What comes through from their suggestions is that they believe people should be charged and go before the courts. In question 14—and we intended this domestically—we asked them whether photo identification should be checked at the gate before boarding, and 77 per cent said that they believe it should be. We did not have anybody from Newcastle respond, where they do do that, but the respondents certainly believe that that should be required.

As I said, it is an ongoing survey. We have to do a correlation between various airports, and the response times—of the APS, for instance; we asked about response times to security incidents—will be more meaningful when they are extracted by airport. We intend to do that when we publish the final report, probably by the end of November. Those things will be able to be gleaned fairly significantly from this report. It is an issue that is of worldwide concern. We followed a survey that was done pre September 11 in the US and we can compare very closely the results of that survey with our survey. Interestingly, in question 3 the percentages of incidents are very similar, save that the survey that was done in the US showed that 42 per cent of respondents had been physically assaulted.

ACTING CHAIR—Thank you, Ms White. Firstly, what sort of airport staff are your members, compared with other unions? Secondly, what additional training have your members received since 11 September 11 2001?

Ms White—Our members work primarily in passenger customer service, and clerical, administrative, operational and supervisory type functions. At an airport, that will be the check-in person, the person who does the weight and balance on an aeroplane or the person who sits in

an office who directs where the aircraft should park. There will be duty managers who supervise and there will be people who work with the crew who come off aeroplanes. That is in larger airports. At smaller airports some of them may very well direct the plane—say at Coolangatta or somewhere like that—and communicate between the company and the pilot. They do those sorts of things.

ACTING CHAIR—Have they received any additional training since September 11? I am thinking particularly of people who have direct dealings with customers rather than people who are directing things from offices.

Ms White—Not as a general rule, no. At Qantas there was a program to be put in about air rage, but that was more a customer service focused thing rather than dealing with conflict.

ACTING CHAIR—I was thinking about other areas as well, not just air rage. People who are working on a check-in are usually the first people that someone walking into an airport has contact with. We heard earlier from a witness from Melbourne Airport that those staff are the responsibility of the airlines and that whether or not they have done additional security training since September 11 is up to the airlines. I presume that a lot of those staff are your members.

Ms White—My inquiries indicate that there has not been any additional security training in the carriers that we cover. Our members include 33 of the overseas carriers, plus the major domestic and regional airlines. The inquiries I made do not indicate that there has been any specific additional security training.

ACTING CHAIR—Presumably if someone is getting aggressive before they are even on a plane, commonsense would tell you that they are the people who are more likely to give you trouble once they have boarded. But you are saying that your members have no support in dealing with those people. What about in denying them access to the flight? If they say, 'I'm sorry, you are too aggressive. You are too drunk. I'm not going to put you on an aeroplane,' is that supported and encouraged by the airlines or is that discouraged because you get unhappy customers?

Ms White—In the main it is probably discouraged. The level of support will vary from manager to manager and it will depend on the sort of incident. As you will see, there are frequent sorts of incidents. We did ask about what the management support was and whether people were put on the plane. More often than not, they are put on the plane. There is a culture of not complaining about it, because there is some sort of expectation that nobody is going to do anything about it anyway, so it is just par for the course, which is a fairly frightening concept. In extreme cases they would be refused access to the flight. Certainly there is an obligation, if a person is drunk, not to let them board an aircraft.

ACTING CHAIR—Would you say that that attitude has changed over time? Have we improved our attitude to people not travelling when they are very intoxicated?

Ms White—I think it is improving. But alcohol is served in airports and in airport lounges. If you were really serious you would not do that at all. You would not give people the opportunity to purchase alcohol in a delay situation or get it free in a Qantas Club or similar lounge. That may be the proof as to how serious we are.

ACTING CHAIR—Mr Lipman, do you want to tell us a little about your experiences? I notice that you have worked for Qantas for 32 years.

Mr Lipman—Security is only as good as your last or most recent incident. The last incident I had was on 27 July. A passenger who was travelling on a foreign airline—Emirates, if I can mention it—managed to get through three security doors in the international terminal and down onto the tarmac. He reportedly hopped into a vehicle and possibly drove it around the airport; we are not sure. No-one actually saw him, but someone saw him getting out of the vehicle around the other side from where my office is.

ACTING CHAIR—Was the vehicle in the place where it was originally parked or had the vehicle been in one spot and you found him getting out of it in another spot?

Mr Lipman—That I cannot confirm, for the simple reason that no-one actually saw him. Where we believed the vehicle was was completely different from where he was seen getting out of it, so we are only assuming that he drove it around or where he drove it. He was noticed by one of the ground transport workers, who brought it to my attention and to the attention of my colleagues in our crewing office, which is in a remote area of the international terminal. We asked who he was, where he was and how he got there. We called our central control to get some security down to our area and it took some time for them to arrive. In fact, I had to make two calls—another call some 15 minutes later to see where they were. Fortunately, he was not violent, but he was not speaking to us. He was in our office and he was trying on coats and so on. We let him so as not to alarm him. Finally, the APS arrived and, five minutes later, the Federal Police.

Fortunately, the Australian Federal Police were able to take control of the situation. But what amazed me was not the errors that may or may not have been made by individuals but the fact that it took so long for a response and the fact that he was able to get through three alarms which were acknowledged—and I believe at the time there were some 30 or 40 other alarms going off. This is the type of thing that could happen with a terrorist: they might create diversions. We were just fortunate that he was not violent and that we were not injured in any way.

I was fortunate that I had been with the company for 32 years and had been through most of the departments at the airport and knew who to report to immediately. But there is a distinct lack of training for all ground staff, I believe, as to proper procedures and basic responses. A basic diagram of the whole airport is also needed so that you can say to security, 'It is happening in area so-and-so,' and they can look at it and say, 'That's the Qantas crewing office,' or 'That's the Emirates load control office,' or what have you. The APS were not sure where we were and quite a few others were not quite sure exactly where our office was because people use different terminology.

ACTING CHAIR—There is no proper map?

Mr Lipman—There is no consistent map or guide. Over the years there have been other incidents—and that is going back a while—but, to me, our individual security is not very good when we are in an office on our own. We need to have more support from the authorities. I find it amazing that someone can come down through three doors, get onto the tarmac, walk around,

drive around or whatever and get to another area and that it takes 35 minutes before he is really seen or apprehended by anyone in authority such as the APS or the Federal Police.

ACTING CHAIR—Is this Melbourne or Sydney?

Mr Lipman—Melbourne.

ACTING CHAIR—You have mentioned the issue of other alarms going off at the same time, and that is something that people have raised with us before. People have said that there are too many things expected at the same time of the APS people at the airport. Do you think they are not allowed to focus clearly enough just on security, that they are doing too many other tasks?

Mr Lipman—I cannot really comment on that because I am not directly involved with their deployment or otherwise. It would appear to me that we need to have once central point in the airport to go to rather than our going through Qantas, Emirates going through their management office and Menzies going through their management office, and then to APAM and APS. We need one central point where we can get quick action.

ACTING CHAIR—Is there not a phone number that you can ring; is there not one security number to get attention?

Mr Lipman—Not that I am aware of, not that is displayed. I know there is a number to ring the APS and there is a number to ring the Federal Police, but the point I was making about the other staff was that it was all very well my being there, but had I not been there my colleague who was there and who is not quite as experienced as I am may not have known exactly what to do or who to ring. I do know, because I did not ask him, but I think that is where we need ongoing training—a briefing once a year even—just to let people know. It is all very well telling us to be alert and to watch out for suspicious things, but I think we need a little more particularly so that those who are on the floor—those who are out on the tarmac, walking around aircraft and what have you—know straightaway who to go to if they see somebody who is strange. I also think that areas should be designated much more clearly.

ACTING CHAIR—If there were a security incident at a gate lounge, for instance, would your average internal phone there have a security number displayed next to it saying, 'In an emergency, ring this number'?

Mr Lipman—On some of them, yes. Out on the aerobridges there is a list up of emergency numbers to ring. You cannot get through on an outside line; you have to go through a switchboard and then ask to be put on an outside call, which I guess is fair enough. If we use our tie line on the Melbourne airport's phones, which are the ones at the lobbies and so on, you get only 25 seconds and then they cut you off. You could be ringing for 10 or 15 seconds for someone to answer and then, when you are halfway through your message, you could be cut off and have to call again.

ACTING CHAIR—Why is that?

Mr Lipman—You would have to ask APAM about that—whether it is something to do with tying the phone up for too long—but I cannot see why that would occur.

ACTING CHAIR—You do not have panic buttons anywhere—emergency buttons that people can press during a security incident?

Mr Lipman—Not to my knowledge, no.

ACTING CHAIR—If you have them and you do not know about them, they are no good anyway, are they?

Mr Lipman—No. Years ago, in certain areas, particularly where there was cash involved—such as at sales desks and even down in the crewing office, because there is money there for crew allowances—there used to be a panic button, but no more. It has not been there for quite a few years.

ACTING CHAIR—Okay. Thanks.

Senator WATSON—Looking at the analysis of your survey on air rage, I notice that Sydney airport has far fewer incident reports than Melbourne airport, although I believe Sydney would have a much greater volume of passengers. Why the discrepancy? Are they a lot more lax in Melbourne, or do you not have as many members in Sydney? There must be a reason behind that. It just seems an interesting statistic.

Ms White—There is a reason. The volume of responses from Melbourne was very large, and it has been smaller in Sydney. We debated whether to give you this as it stands—we are currently working on Sydney. There have been fewer responses, but I am confident that Sydney will be the same as Melbourne. We should have the results by the end of November. Our membership is very high at Sydney domestic and Sydney international airports.

Senator WATSON—But to me that would suggest that there were fewer problems, so Sydney must be coping better than Melbourne. Would that be the right interpretation?

Ms White—No, I do not think that is an inference you can draw. It is about who went out and asked people whether they wanted to fill in the survey, and we have not done as much work in Sydney as we could have done.

Senator WATSON—So it is a bit misleading.

Ms White—It is not misleading, in that it reflects the fact that there are about 3,000-odd customer service agents in Australia working for a range of airlines and ground handlers and it is still statistically a significant percentage who have replied. We have not extracted the information by airport and we will do that, and we intend to get more statistics from Sydney. The reason that the response has not been so big in Sydney is because the key people who would distribute the survey have been away, and so that makes it difficult for us as an organisation.

Senator WATSON—I see.

Ms White—But, again, we have represented these as preliminary findings. We intend to issue the final findings in November.

Senator WATSON—In the survey, one of the suggestions by a respondent from United Airlines at Melbourne airport is:

No cars should be allowed to drop off or pick up passengers …

Ms White—Yes.

Senator WATSON—Another one, also from United Airlines, suggests:

No cars or buses should be at departure level.

Wouldn't that make it pretty impractical or very inconvenient for people to get from a car park or somewhere else to the departure zone?

Ms White—It would make it inconvenient, but I think they—

Senator WATSON—Do you discuss the reasons for that in the survey?

Ms White—I understand the reason for that. The reason is that frequently cars are left out the front of airports. You will see—

Senator WATSON—That is a separate issue. There are two issues that these respondents raised: no cars should be allowed to drop off or pick up passengers; and cars should not be left unattended. I have not asked about leaving cars unattended; I understand that one. But having no cars pick up or drop off passengers and having no cars or buses at departure level seems pretty draconian to me, because they are well away from the planes. What is the difference between a bus stopping outside Myers in Melbourne and a bus stopping outside an airport departure gate, well away from the planes?

Ms White—I guess that airport workers saw September 11 as fairly significant. You would also be aware that the most recent hijacking emanated from Melbourne, so the people at Melbourne airport are probably more sensitive to the potential for bad things to occur at their workplace. It is just a suggestion that someone has made. They say 'departure level'; they may mean that the arrivals level would be a better place. We have not questioned each of these respondents; we have put down verbatim what they said. It is for the authorities to accept or dismiss what the employees at the first line think about it.

Senator WATSON—I was just thinking that they are fairly impractical for older people—lugging cases from a car park or from arrivals level, up to another level, just to check in.

Ms White—They must have had a reason for it. There must have been buses. I cannot be in the mind of the person who filled that in, but I do know that people have been concerned about cars being left unattended. Their concerns are that we do not live anymore in a world where, at an airport, you can feel safe if somebody's car is left and they are paged for half an hour about it being unattended. I guess it comes from that. There is a family in airlines, and United Airlines had two of their aircraft slam into buildings, so they would be more sensitive to that than, perhaps, other airline workers. It affected their airline significantly. Their airline went into chapter 11 and they understand what significant security breaches can do.

Senator WATSON—Are they asking for more than is practised in the United States? If it is reflecting what has happened in the United States I can understand the feeling, but are these people asking for more, in terms of security—that no cars or buses be able to drop off and pick up passengers?

Ms White—They may very well be asking more.

Senator WATSON—You do not know?

Ms White—I do not know.

Senator WATSON—You say we should have one single federal law in Australia to prosecute airport offenders. Would that be difficult? There is such a range, from Sydney right down to remote airports. Do you have problems with state police being able to apprehend people?

Ms White—The number of people who have been prosecuted for offences and assaults is very small.

Senator WATSON—Yes, I gathered that.

Ms White—That is not only from this survey but generally. If an offence occurs in the air—and I understand why it is Commonwealth legislation—why is it not as serious in an airport? Why shouldn't there be one single law so there is no confusion about what applies, who should do it and who should enforce it, so that it is really quite straightforward? The US adopted it as part of their parcel of legislation and that is not a bad benchmark for us, we think.

Ms KING—Mr Lipman, with regard to the incident on 27 July you were referring to, were you involved in any debriefing about that incident?

Mr Lipman—Unfortunately, no. All I have seen is a copy of the debriefing which was given by Melbourne Airport. But, no, I had no debriefing. Four days after the incident I was called at home and asked if I wanted counselling, but it was a bit late then. There was no debriefing. To find out any results, I had to do a little bit of fishing myself, to find that this person who was involved ended up in the psychiatric hospital at Broadmeadows—I do not know whether he was deemed to be unfit or mentally ill. But there was no debriefing.

Ms KING—You obviously did a pretty brave thing: challenging someone who you thought should not be there. Often, in secure environments—as I know myself—if you go through a door and someone else happens to follow you, you may notice they do not have a security pass on but it is quite difficult to actually challenge them and say, 'Excuse me, what are you doing in this area and who are you?' Is there a culture of people challenging people in these areas or is it just that you were particularly vigilant?

Mr Lipman—I think it is just vigilance. I do not believe too many people would challenge when on their own. I may have had second thoughts if I had been on my own, but there were two other people around and I felt more secure. But it is not an easy thing to do, on your own: to challenge someone when you do not know how they are going to react. By all means, ask what

are they doing there et cetera, but what are you going to do when that happens and you need help straightaway? That is the important issue.

Ms KING—What if he had been able to give a reasonable explanation for being there—he was a contractor going into Customs to get a mainframe or something?

Mr Lipman—If he has no identification, no ASIC, for a start, he should not be there; it is unlawful totally. That was the first thing. When there was no ASIC we felt: 'Right, this is a job for the APS.'

Ms GRIERSON—You commented on air rage. Do staff talk about recurrent offenders? Are there serial offenders travelling on our airplanes?

Ms White—In my experience they talk about well-known people who are serial offenders—celebrities. You thought I was going to say 'politicians'. The results are not yet in from Canberra; they might make quite interesting reading.

Ms GRIERSON—We look forward to that.

Ms White—That is what they seem to talk about.

Ms GRIERSON—Is there a reporting process if you are aware of someone who seems to breach etiquette and protocols regularly?

Ms White—My understanding is that they can mark a person's file if they have done something. That will alert them. I think there is a set of codes—they may be an unofficial set of codes—for marking people so that they are warned in future.

ACTING CHAIR—You can always send their bags to Switzerland when they are going to Canberra!

Ms GRIERSON—Airports do have security plans in place. One would expect that occupational health and safety committees would be involved in those plans. Are your unions represented on the committees in the process of monitoring, developing and implementing these plans?

Ms White—Yes, we are involved in the airport committees. Mr Stanley was a member of the Melbourne airport committee and would have some input into it. They do not meet as regularly as you might want. We also have with each airline occupational health and safety committees, which meet and raise issues. The ASU has a national one, and we raise issues. They have local committees too. There is a regime of occupational health and safety to raise these issues. It is one thing to raise them with your employer but if it is the airport which is responsible for how things operate then the matters have to be raised with it and then the chain drifts away from you. That is why in Mr Stanley's case he did an assessment basically of the airport from their point of view which went up the chain, but they could not influence their employer because their employer has to influence—

Ms GRIERSON—Do you think staff are being adequately trained in, and offered training in, conflict resolution and basic protective behaviours?

Ms White—No, I do not think so. I do not think it is adequate. I do not think there is recognition that it is an aggressive place up there. It is pretty much brushed under the carpet. When we have raised it there has been reluctance to provide training other than training of a customer service soothing type rather than addressing: 'What are we going to do? What are the procedures? This is wrong. This is what we should do.'

Ms GRIERSON—How extensive is video surveillance in most airports?

Ms White—I am unable—

Ms GRIERSON—Perhaps I should ask someone else that. I will do that. Your members who responded to your survey have lots of suggestions and there was some mention of undercover security. Is there ever undercover security present? Are you aware of undercover security being used at times in airports?

Ms White—I am not aware of undercover security at airports. Only the air marshals are undercover, as we are aware. I am not aware of any undercover security at airports.

Ms GRIERSON—They mentioned some fairly basic preventative measures. I suppose one of those is penalties. Do you have a view on penalties for aberrant behaviour or aggressive behaviour by passengers?

Ms White—Certainly we believe that in extreme cases imprisonment is not out of the question for physical assault. The concern we have is that it actually never gets there. It is, as we say, part and parcel of the job. What we really need to get over is a hurdle. We think the deterrent value of actually enforcing it will probably reduce the amount of air rage that occurs. The penalties now probably are the normal assault penalties or the normal abuse penalties, but that just does not happen.

Ms GRIERSON—Perhaps there is a heightened safety environment. Are there emergency buttons and panic buttons in major airports? Do they make sense as a deterrent? Is putting them in warranted? Would you get the response that you want?

Mr Stanley—There are emergency buttons in certain locations. I have found that the response to them is very bad. The emergency buttons can be hit but there is rarely a response from the private security firms at the airport.

Senator WATSON—Really?

Ms GRIERSON—So the staff suggest in these surveys that they would like to see more APS and AFP presence in airports but they are also critical of response times and the sorts of responses.

Mr Stanley—The particular alarm buttons that I have mentioned are not directed to the APS. I am sure they are directed to the private security firms that Qantas employs at their terminals. I do not think the APS is linked to them.

Ms GRIERSON—Is there a preference for the APS rather than private security firms? Is there a view on that, or any performance results?

Ms White—People want somebody who can take action and follow it through rather than just scold the offender, and they want it to be clear to people that that is what will happen. That seems to be the flavour of the results. We do not want a person to be able to walk away from an incident which we regard as serious.

Ms GRIERSON—So you want more instant access to, and visible presence of, security officers as a deterrent?

Ms White—The desire for a visible deterrent was highlighted in the survey. People want to see security out there. They believe that people are less likely to behave badly when they see someone who is likely to stop them. That is clearly what is being said.

Ms GRIERSON—I think people are becoming much more aware of unattended baggage and unattended cars as a risk. Do you see any move by airports to control these in any way?

Mr Lipman—From my observations over the last few years, particularly after September 11, there is a conscious effort. Any bag that has been sitting unattended is reported straightaway and is attended to very promptly. As far as cars on the roadway are concerned, I know that traffic officers are out there moving them on quickly, and they are pretty quick to pull out their booking pad and put a ticket on them. But concerning the moving of unattended cars you would probably have to ask the airports.

Ms GRIERSON—Reading your submissions, I get the impression that staff feel too removed from the security process.

Ms White—That is the reason we have highlighted this. Our view is that you are only as good as your last incident. We have highlighted this incident at Melbourne airport not because it is the only incident or because we are meeting you in Melbourne but because staff want to see something come from it. This is an extreme incident.

Ms GRIERSON—There were so many breaches.

Ms White—There are so many breaches. As a result, I do not think there is a feeling that there is an involvement—looking at the involvement of the staff in this incident and the fact that they were not debriefed. They were not involved; they gave their statements but they were not asked. Mr Stanley did the occupational health and safety audit off his own bat because his colleagues felt bad about it. There was not anything that really brought them into the picture to give their valuable contribution.

Ms KING—Mr Lipman or Mr Stanley, has anything changed that would lead you to feel confident that the incident that happened on 27 July would not happen today?

Mr Lipman—From my perspective, no; I cannot see anything concrete that would change my view at the moment.

Mr Stanley—I would tend to agree. I do not think we have made any leaps forward. I think we are still in the position we were in at the time. There may be some more undercover surveillance, but certainly it is not visible—we are not aware of it. We have not been made aware of any changes to the procedure.

Ms GRIERSON—You are a union representing people across a wide variety of locations. There have been some submissions to the inquiry that suggest that costs at regional airports are very high. Therefore, there is an inference that levels of pay would be different in regional airports than major city airports. Do you have a view on that?

Ms White—We believe that people are paid for the skill that they exhibit and that they perform. The skill they have should not depend on where they live. We believe that somebody who performs a vital security function at Tamworth, Gove, Port Hedland, Alice Springs or Ayers Rock should not be paid less than somebody who does it in a major capital city. We think that their work is as valuable as their city colleagues.

Senator WATSON—I was amazed by an answer you gave a colleague a moment ago that there had been no heightened training as a result of September 11 so far as your membership was concerned. Did I interpret your answer correctly?

Ms White—Yes; I am not aware of any security at airlines that has been more significant since September 11.

Senator WATSON—We have been told about heightened training et cetera, but is it just with pilots and—

ACTING CHAIR—Screening staff.

Senator WATSON—and those sorts of things? From the point of view of your members—

Ms White—From the point of view of our members, no; the focus has been on pilots, flight attendants and screeners. If you look at the figures of what has been expended, that is where the money has been.

Senator WATSON—Give us some idea of the sorts of important jobs that your people do where you think that heightened training or improved training is necessary.

Ms White—They check people in. They are the ones who check that they are who they say they are at check-in. They ask them the questions about whether they have had their bags packed properly if they are travelling internationally. They look at the demeanour of people. They are the first point of contact by the airline with a passenger.

Senator WATSON—What about your other members—does that cover baggage handlers?

Ms White—No, we do not cover baggage handlers. We only cover clerical and administrative people—for instance, we have duty managers. People who are supervisors and managers—where incidents get escalated to—are our members as well.

Mr Stanley—We have a rather large lost baggage department. We reunite baggage with people when it is mislaid. We represent a lot of people in that area.

ACTING CHAIR—Do you think that there are security issues for people in the lost luggage area?

Mr Stanley—They are the first ones called when there is a suspicious bag. Usually they are the first ones who are alerted by the baggage handlers, as you said earlier. If there is a suspicious bag left on the carousel, they are the first people called. They have to get some security people in that case. So there are issues for them—definitely.

ACTING CHAIR—Mr Stanley, we have had a really good go at questioning Ms White and Mr Lipman. Was there anything that you wanted to add?

Mr Stanley—No; I am quite happy with the people that are here and I am quite happy with anything they said. I think we were reasonably well briefed on what we were going to talk about. I am sorry I was late, but unfortunately I had no choice.

ACTING CHAIR—That is fine. We have covered a lot of ground and I just wanted to make sure that you were not missing out. I thank the representatives of the Australian Services Union for appearing before us today. If we have any further questions, I hope you will not mind if we put them to you in writing.

Ms White—That will be fine.

ACTING CHAIR—Thank you very much.

[12.18 p.m.]

REID, Mr Peter Julian, Engineering Manager, AACE Worldwide Pty Ltd

ACTING CHAIR—Welcome to the hearing. We have had a submission from AACE Worldwide. Do you wish to present any additional material or make a brief opening statement to the committee?

Mr Reid—I have no additional material, but for everybody's benefit I will quickly summarise the submission. We believe the layered approach to aviation security that is now in place can be extended one step further—that is, by protecting the cockpit or flight deck. I will use the words interchangeably.

Senator WATSON—Excuse me, what do you mean by the 'layered approach'?

Mr Reid—The layered approach is that the check-in people look at your demeanour and they ask you whether you packed your own bags. That is the first layer. Your bags go through X-ray, you go through X-ray and all your carry-on baggage goes through X-ray. There are continuous layers. There is a proposal to make it go further, to see if you are an acceptable person to fly. You could follow the American tradition and have a big database with everybody on it. You get points or colours for your coding. So there is a layered approach to trying to remove security threats from airlines. It starts right back with passports, passport control, photo ID and all those issues. From a systematic point of view, there is a layered approach: if you get on the aircraft, you have gone through a series of checks before you get there.

There is a need to install a last layer, which is protecting the flight deck from anybody who has the intention to take control of the aircraft for whatever reason. Australia has not implemented that as a regulation. The US has. We believe that it is partly to do with the structure in Australia, where the Department of Transport and Regional Services and CASA have conflicting requirements and they are not under the same management, as against the FAA in the US.

The other thing that we believe can improve the handling of a hijack situation, if you get one on an aircraft, is the installation of video surveillance and wireless notification devices so that the flight crew know about the incident. During the last incident with Qantas there was a period of time in which the flight crew did not know what was going on. We believe that there is a need to take this layered approach to the next level. We are a manufacturer and designer of these products, so we obviously have a particular vested interest, but we believe they improve the whole security apparatus for the airline industry and prevent the use of aircraft as weapons.

Ms KING—I note from an inclusion in your submission to the committee that you wrote to the minister for transport quite some time ago and received a response, I think, dated almost a year ago. Are you surprised at how long it has taken to do anything about cockpit security?

Mr Reid—We are, in two senses: there has been neither a positive nor a negative response and there has been no justification for the lack of response. It is, if you like, a conceptual costing

issue. We know that airlines are reluctant to do this because it adds somewhere between $US30,000 and $US50,000 per aircraft to the cost. It takes the profit off their bottom line and, given that the airline industry is not that healthy at the moment, airlines are reluctant to do it.

ACTING CHAIR—Does that add to the cost of constructing a new aircraft or does it add to the cost of modifying an existing one?

Mr Reid—Modifying an existing aircraft. It will be included in the cost of a new aircraft. It goes back to when you start to actually build the aircraft. Any aircraft that came off a production line before last April will need a retro fit, so it will have to go back. The addition to the cost of a new aircraft is probably a lot lower—probably down near the $US10,000 mark—because the doors are much more secure. Existing doors are basically honeycombed. New doors have Kevlar and aluminium and all sorts of security features in them to stop bullets, which are extremely hard to stop.

Senator WATSON—I query whether there has been no change, because I have noticed there are different sorts of doors on some aircraft. I wonder whether you were really correct in saying that there has been nothing happening.

Mr Reid—The US mandated from 9 April this year that all aircraft flying in their airspace had to have what are called phase 2 doors fitted. So any airline that operates into US airspace—and Qantas is a big operator into US airspace—

Senator WATSON—I am talking about domestic planes.

Mr Reid—Qantas have taken a fleet decision that they want to have total flexibility in their allocation of aircraft. In essence they have decided that if any airline needs to fly to US airspace it needs to have these in, so they are installing them in their whole fleet. Other airlines who fly into Australia and do not go into US airspace will not have fitted them. New aircraft will have them, because the manufacturers will deliver them. So Qantas's latest airbus, the Airbus A340, has a new secure door, but old aircraft do not.

Senator WATSON—No old aircraft have them?

Mr Reid—Some of the older Qantas ones do, such as the 747s that Qantas fly that go to US airspace.

Senator WATSON—I am talking about planes that just fly domestically.

Mr Reid—Not that we are aware of. Qantas have a program to roll them out into the 737, which is their main workhorse for the Australian market. Virgin, as far as we know, have not committed to rolling them out yet. They may well have made a commitment, but that would be a commercial decision.

Ms GRIERSON—This may not be something you can answer, but obviously the costs of these things are a disincentive to the airlines. However, they should translate to reduced insurance costs. Have you any knowledge of that?

Mr Reid—I have not any direct knowledge. When you work on aircraft you have to get insurance, so I have been talking to insurance brokers. I do not think it would make that much difference to their insurance costs because in essence if they cannot get through the door they are going to blow up the plane. The total cost to the insurance companies is the same if they crash it and kill all the people or if they blow it up and kill all the people.

Ms GRIERSON—All right. So you are making recommendations that cockpit security systems and flight deck security systems should be installed—and obviously you are a provider of that sort of equipment. Do you have a view on which planes and which routes should incorporate those?

Mr Reid—Basically, all planes because they can all be used—anybody who flies near a major metropolitan area, be it here or overseas. Because of the approach in Australia it is probably unlikely that an Australian aircraft would be subject to this sort of terrorism but Australian aircraft fly through ports that have not got as high a level of security as we have in our airports. There is a higher chance that an Australian registered aircraft could be used for this overseas because our aircraft go to an awful lot of places.

ACTING CHAIR—Would you say that it was more of an issue for aeroplanes travelling on international routes or are you advocating that these doors should be fitted to planes on domestic routes as well? Where would you stop? You do not want them on light aircraft, presumably.

Mr Reid—If you wanted a rule that was staged, you would fit it to aircraft flying on international routes. The implication is if Australia introduces that rule it means all the aircraft flying to Australia have to have it fitted because it is our airspace. That is why it has trade and foreign affairs implications. With the Americans, they just arbitrarily said that every aircraft has to have it. Every airline that flies in American airspace has to be fitted with these doors.

We had discussions with the Pakistan International Airline and they fitted part of their fleet, so they now have a restriction on how they can schedule aircraft. The ones that go to American airspace have the doors fitted and they are waiting on approval for a more cost-effective solution to do the rest of their fleet.

ACTING CHAIR—Are there any countries besides the United States that have this similar requirement?

Mr Reid—It is in an ICAO requirement for implementation by November this year, but that requires national authorities to mandate it. As far as I am aware, nobody else has mandated as a national authority, but it is very hard to keep up.

ACTING CHAIR—So it is a recommendation so far?

Mr Reid—Yes. Everything from ICAO is a recommendation.

Ms GRIERSON—Has the US mandated any flight deck security systems or measures?

Mr Reid—In what respect?

Ms GRIERSON—Any surveillance within cabins or—

Mr Reid—No, they have not.

Ms GRIERSON—So only the cockpit door?

Mr Reid—Yes, only the cockpit door.

ACTING CHAIR—Do they have undercover security travelling on American planes like we do?

Mr Reid—They have air marshals.

ACTING CHAIR—Are they undercover?

Mr Reid—Yes.

Senator WATSON—It is an exercise in semantics when you correctly report that DOTARS is responsible for aviation security and CASA is responsible for aviation safety. Where we have two regulators in this line, how do we know that something might not slip through the safety net?

Mr Reid—We do not. That is the issue. Security and safety in the aircraft industry have totally different meanings. Safety is making sure that if you go in a plane you get to the other end and get off again. Security is about stopping people taking control of planes or shooting you. You might be safe as far as the aircraft is concerned—in other words, it is a nice safe aircraft that will take off and get down all right—but it may not be a secure aircraft; in other words, they might not keep the ratbags off. In that case the plane is safe but it is not secure. It is a distinction. The grapevine suggests that this is a real problem between CASA and DOTARS.

ACTING CHAIR—In what way?

Senator WATSON—Can you tell us a bit more?

Mr Reid—Because they interact. If you put a security door in, you change the actual structural integrity and the safe operating of the aircraft. It has been put in for a security reason but it impacts on the safety of the aircraft and you have to resolve both those issues. Having a dual regulatory environment means that there is nobody really responsible other than the minister.

Senator WATSON—Can you give us instances of where there have been problems of interpretation between DOTARS and CASA?

Mr Reid—I believe that not having made a decision on security doors is an incident that has the highest meaning. Other than that, because it is all internal and bureaucratic I cannot actually give you either any anecdotal or in camera type responses.

Senator WATSON—So you would like to see one body responsible for both safety and security?

Mr Reid—Yes. I believe they are so intertwined in today's environment that a single regulatory authority to manage airline security and safety is required.

Senator WATSON—Yes, that is a good point.

ACTING CHAIR—Another suggestion that you have put is that video surveillance or wireless threat notification devices be fitted to passenger aircraft. Would they be cheaper than the doors?

Mr Reid—Yes.

ACTING CHAIR—How much cheaper?

Mr Reid—It depends on what degree of video surveillance you want. A security door, because it has a structural impact on the aircraft, is much harder to get approved whereas wireless threat devices and the video surveillance devices are add-ons, so you are probably looking at a quarter to a third of the cost to do it.

ACTING CHAIR—By wireless threat device you mean a panic button, don't you?

Mr Reid—Yes. The reason to go for a wireless threat device is that it can be a fob key, so the cabin crew can press it without that being noticed by the potential hijacker.

ACTING CHAIR—Is this something that they would wear?

Mr Reid—Yes, or they could carry it like a standard key. Nowadays it is the same size as a car key. They carry it on themselves and they can press it. It can be around their neck or whatever approach is taken. The idea is to alert the flight crew that something untoward is going on and then they can take the appropriate action and request the authorities for clearance to land or to change tack.

ACTING CHAIR—How does it work? If you activate a threat device, does it make a noise?

Mr Reid—You specify how it behaves. The design that we believe is the most appropriate has a recessed button so it cannot be activated accidentally; there has to be a definite action to activate it. It makes no noise on the person who activates it. It raises the appropriate alarm levels in the cockpit for the flight crew. If they have video surveillance, they then survey the aircraft and see what the issue is. A threat could be just drunken rugby players, which seems to be a common tactic at the moment, or rugby supporters. It could be something like that, so it is not to do with hijacking; it could be because the crew need police to be there when the aircraft lands. So it is rather than the crew having to make phone calls. There have been reports in previous hijackings of cabin crew being assaulted because they have reached for a phone. It eliminates that threat.

ACTING CHAIR—Or it reduces it. If there is an edgy terrorist with a weapon, they would probably not be too happy about you putting your hand in your pocket.

Mr Reid—But it is a wireless one and all the cabin crew have got it. It is a lot harder for the potential hijackers to survey and keep track of all the movements of all cabin crew. Also, phones are only every 20 metres in a plane.

ACTING CHAIR—One of the other submissions that we have received suggested that an overt security presence acts as an effective deterrent on aircraft, whereas the sorts of things that you are talking about are not so in your face. Do you think that we are better off spending money on air marshals? Why should we go the way that you are suggesting?

Mr Reid—Unarmed air marshals, yes—but I believe that armed air marshals are a safety hazard because their arms can cause decompression in aircraft, which probably has a higher risk of causing problems than hijackers, in one sense.

ACTING CHAIR—Unless the marshals are armed with fasers.

Mr Reid—Yes, that is right, but then they have to get up personal and close. I believe there is a case for both. Obviously, 'no entry' and 'no smoking' signs are overt and everybody can see them, and that sends a message. I believe that also should be done here, so it is a combination. As the previous witnesses said, I think there is a need for high-profile charging of people who cause trouble on aircraft. It sends a message to the general public. A lot of these problems may be because the people who want to hijack and terrorise can hide behind general bad behaviour on aircraft.

ACTING CHAIR—One of the themes that has come up a few times is that if you are a terrorist now you would not bother hijacking an aircraft because there are plenty of other civilian targets. You could walk into Town Hall Station in Sydney with a bomb in your suitcase and do a lot more damage a lot more easily than by hijacking a plane and flying into something. Do you think we are trying to shut the gate after the horse has bolted? Instead of concentrating on potential new threats, we are concentrating on the threat—

Mr Reid—The fighting the last war syndrome?

ACTING CHAIR—Yes.

Mr Reid—I think the most obvious threat at the moment to Western infrastructure is petroleum trains. If you hijacked one of those and put explosives on every carriage you could create a whole heap of havoc. Being an engineer, I can think of heaps of ways to terrorise a community. It really depends on your mindset as to whether you implement any of those. The only big threat we still have left in the aviation industry is hitting a nuclear reactor or power station with an aircraft, which is probably the only way to attack those environments. That would create all sorts of havoc. They have good security at ground level, but they really do not have good security in the airspace.

Senator WATSON—What sort of plane would you need to make a difference to, say, Lucas Heights?

Mr Reid—Some of the bigger ones—the A340s and Boeing 747s. I am not a nuclear regulatory expert or engineer, but my understanding is that the containment things on nuclear reactors were designed to withstand the impact of a 707, because that is what was new when they were designed and built. Any plane that is bigger than a 707 will probably have some impact, and when it is a lot bigger—a 747 or an A380, when that comes online—it is extremely likely to do a lot of damage. Even ordinary power stations can mean a lot of damage.

ACTING CHAIR—Thank you, Mr Reid, for appearing before our committee. If we have any additional questions, can we write to you?

Mr Reid—That would be fine.

ACTING CHAIR—Is it the wish of the committee that the document entitled 'Preliminary survey results' presented by the Australian Services Union be taken as evidence and included in the committee's records as exhibit No. 5? There being no objection, it is so ordered.

[12.39 p.m.]

GRAHAM, Ms Pamela, Manager, Operations, Melbourne Airport, Australian Pacific Airports Corporation

ACTING CHAIR—I now welcome the representative from Australia Pacific Airports Corporation back to the hearing. Ms Graham, you have already been sworn in, so we will just ask you a couple of questions. The Australian Services Union raised a security incident on 27 July at Melbourne airport which involved a person going through three security barriers, ending up on the tarmac and possibly driving—but certainly entering—a vehicle on the tarmac. There was a delayed response time of over 20 minutes before security arrived to deal with him. Can you explain to us how that happened?

Ms Graham—I will take you back to the beginning of the incident. It was an Emirates passenger, and he was fairly lively and vexatious during the check-in period. The APS were called to have a talk to him and investigate his behaviour at the time, and eventually it was agreed that he could continue to travel. He then passed into the customs area and went through customs. That was fine; he had all his legitimate documentation. He went through the screening point, as I recall, and he then smashed one of the 'break glass' alarms on the doors that take you down through the stairwell to the apron. Those break glass alarms have to be there for fire safety reasons. They present a bit of a security issue, obviously, because of the ability for people to actually get through the doors, but, by regulation, we have to have them there. He went through the one at the top and then walked down a ramp, down the final stairwell and onto the apron through another break glass alarm, which would have activated in the airport coordination centre. A couple of things happened. There were a number of other alarms that were active at the time—and we discovered later on that there was a cabling issue. When that alarm was activated, it activated some other doors as well down near the customs area. The APS initially responded to the doors leading into what we call the 'arrivals baggage reclaim area', so there was some confusion with the call-out process.

Two issues came out of that. The first was that there had been a very high number of false alarm rates. Unfortunately, some of the staff in the coordination centre had lived with that for some time, and I do not think they had brought it to anyone's attention. Once we were aware that there were so many false alarms appearing on the computer screens at the one time, we undertook an investigation into it. There have been a lot of cabling and technical issues, most of which have now been rectified and there has been a very major reduction in the number of false alarms. The second thing was the cabling issue, and that has been fixed.

We held a major debrief, as we do after all these sorts of incidents—we have a formal debrief with all the people involved. As a matter of course, we invite Qantas, as a major player at the airport, and who they invite to attend the debrief with them is a matter for them to decide. What came out of that debrief were some technical issues in terms of the alarm system, which I have just mentioned.

The APS did respond, but they responded to another area. But we went back and looked at the process of a person coming down from the departures level to the apron level and the time it

would take for them to do that. There are generally two APS officers on the apron area at Melbourne: one is down in the cargo terminal area and the other one is usually up around the international apron because the international apron is the area considered to be of highest risk, which is basically where this incident occurred. It is still a moot point as to whether the APS officer would have got there, and we recognise that. There is the potential for a person to come down and go out onto the apron, and where the person exited onto the apron there is a lot of machinery, equipment, nooks and crannies, and it is quite easy to disappear amongst all the equipment. So, even had everything worked absolutely perfectly, we are not sure whether the APS would have got there on time. We have to assume that they would have.

ACTING CHAIR—You talk about a cabling problem that your staff had been living with for some time. Wouldn't you, as a matter of course, be testing those systems? Why was the problem of false alarms not picked up earlier?

Ms Graham—Good question. I think the system was working in the sense that nothing would have appeared wrong to the communications officer who was managing the system other than that a large number of alarms on a number of doors was being indicated. So it was more volume than the actual system. Certainly when we went in and had a really good look at the system and a number of door forced alarms that were appearing, it was clear that there had to be some sort of technical issue associated with it. But unfortunately it was just one of those things where staff had worked with it for a long period, and had become perhaps used to it.

ACTING CHAIR—I still do not quite understand. If some sort of security control room gets a message that a door forced alarm has gone off, presumably someone goes to check that door.

Ms Graham—Yes, they do.

ACTING CHAIR—Then they come back and say it has not been forced; it has not been touched. Doesn't that trigger a question in the mind of whoever is managing that process that something has gone wrong? I am not quite sure how you could have a number of situations like that occurring regularly and that not lead to some questions being asked.

Ms Graham—I cannot answer that directly. I would have to take it on notice to check whether some of those things were referred through to the technical maintenance people. Whether they were addressed at the time I do not know. I could take this on notice. That is my only suggestion.

ACTING CHAIR—The concern it raises is that you have, presumably, a staff culture developing that assumes that many of these are false alarms. So your response time automatically increases and the need to get to absolutely 100 per cent of call-outs decreases because there is always the question in the back of someone's mind that it is probably a false alarm.

Ms Graham—I do not disagree with that. I think that is true. The responses may have been affected because there was an assumption that things were false alarms rather than real alarms. So I accept that.

ACTING CHAIR—There is not regular testing?

Ms Graham—I am assuming there is regular technical testing of it, but I cannot say what the outcome of that is.

ACTING CHAIR—You say that there is a formal debrief with all of the players involved, but that does not involve the people who are on the front line of the incident, does it?

Ms Graham—Yes, it does. But, as I say, we would go to Qantas and say, 'Bring whom you feel is the appropriate person to the debrief.' Of our own people, we would always bring the people who were actually involved at the time. We expect any organisation that we invite to the debrief to do the same.

ACTING CHAIR—Another issue that was raised is the issue of cars not being removed when they are parked outside the terminal illegally. What action do you take with cars left outside when they should not be?

Ms Graham—There is an additional security measure that says—I am just trying to recall the wording—that after two minutes, if a vehicle is unattended, an effort be made to locate the person by paging. Then, if there is no response to that, within five minutes we have to take some action to assess the vehicle. We call the Australian Protective Service bomb appraisal officer to do that and they do their assessment of the vehicle to ensure there is no explosive in it. They also do a check on the registration of the vehicle. After that process, if there has not been anybody attend the vehicle, we call a towing company to tow the vehicle.

I will be quite frank about this. It is pretty hard to get towing operators to respond to that, because they assume that the person will appear within the time frame that they are likely to respond to it. We have one towing operator—Adams Towing—which are usually our preferred operator because they are likely to respond better, but even they are not always as effective as we would like.

ACTING CHAIR—Do you pay them?

Ms Graham—Yes, we pay them.

ACTING CHAIR—You pay them either way?

Ms Graham—Yes, we pay them a fee to remove the vehicle.

ACTING CHAIR—But, if the owner turns up after you have called the towing company but before they get there, do they still receive a payment?

Ms Graham—I think so.

ACTING CHAIR—A call-out fee would be an incentive to get them there, surely, if that is the problem. Are there any panic buttons anywhere in the airport?

Ms Graham—Do you mean a hot button system?

ACTING CHAIR—A key or a button that you would press to attract the attention of APS.

Ms Graham—There is not a hot button, if that is what you are saying. There are phones. I have to raise the issue of the emergency number. We have for a long time placed stickers on all the phones that have the particular key numbers 'fire', 'first aid'—because we get a lot of first aid incidents at the airport—and 'emergency', with the actual number for emergency. I would have to go back and check every phone to see if there are any phones which have been missed, but that has always been our policy. I think we did a reissue of those stickers only about five months ago, so I would be surprised if there are phones that are missing the stickers. On the apron area, we are actually in the process of installing a hot button system.

ACTING CHAIR—Who will that be connected to?

Ms Graham—That will be connected to the particular coordination centres—like the Qantas coordination centre and our coordination centre.

ACTING CHAIR—Not directly to security?

Ms Graham—Our coordination centre is also our security control centre.

Ms GRIERSON—The reason for this inquiry was that the Audit Office did actually go through several alarmed doors at airports in Australia and they had no response to those breaches. So that is why we are here. That was quite some time ago, so I suppose it adds to the committee's concern that more recent incidents have been reported to us. Is your security coordination centre manned by staff or a private contractor?

Ms Graham—Can I just explain something about it. It is not just the security coordination centre.

Ms GRIERSON—No, it is your whole communications, operations and everything else.

Ms Graham—Air side safety, apron safety; it is the coordination centre. It is manned by our own staff.

Ms GRIERSON—Are roles defined for those people?

Ms Graham—Absolutely.

Ms GRIERSON—Is there one person who responds to alarms?

Ms Graham—Yes, one person.

Ms GRIERSON—Who are they accountable to?

Ms Graham—They are accountable to the terminal manager.

Ms GRIERSON—If they need someone to go and inspect it, is that done by a private contractor or staff?

Ms Graham—It is Australian Protective Service staff.

Ms GRIERSON—But you only have so few of them there.

Ms Graham—That is right.

Ms GRIERSON—Are you suggesting that there are not enough?

Ms Graham—You would always like more security patrol staff.

Ms GRIERSON—So should you employ more yourself?

Ms Graham—We have apron safety staff who supplement the APS, but their prime role is really safety.

Ms GRIERSON—Would you recommend that more APS staff be provided to airports, or do you think that cost is something you should bear?

Ms Graham—We would like to see more APS staff provided.

Ms GRIERSON—I think that is probably something the union and the management would agree on.

Ms Graham—Can I just go back to the point about the alarms. No matter how quickly you get down to the apron—and, as I said, we did a simulation on this—you still have to have the people to respond on the apron.

Ms GRIERSON—In relation to the situation of the recurrent alarms and the high rate of false alarms turning out to be a cable problem, do you think your maintenance procedures are organised in such a way that security is a priority?

Ms Graham—I think they are now.

Ms GRIERSON—You said that Qantas decided the extent of, and who should be involved in, that debrief. Do you think that is an abrogation of responsibility?

Ms Graham—No, I certainly do not. There is a tendency for the airport operator to be seen as the be-all and end-all for security. Everyone has got to play their part. We are a staff of 160 people. If we go to Qantas and ask for representation from Qantas, we expect Qantas as an appropriate manager of employees to know who they should send. Quite clearly, it is up to them to decide that.

Ms GRIERSON—I would suggest to you that each player would have a vested interest. You would have overall interest in everyone getting it right—

Ms Graham—We do.

Ms GRIERSON—and therefore you should have a greater interventionist role in those sorts of issues. Would you like to comment on that?

Ms Graham—We have a very strong interventionist role but, at the end of the day, the particular person was an employee of Qantas, and we would expect Qantas to accept their responsibility in ensuring that the right people were at the debriefs. There is only so much we can do. We can lead people to the water but we cannot do everything. I think there is a tendency at the moment to expect airport operators to take on all the responsibilities for security. and clearly we are just not able to do that. We are certainly willing to coordinate it and to take a leading role in it but not to be the overall supplier of security services.

Ms GRIERSON—If you are going to coordinate it, that gives you a major role in knowing all of it and making sure all of it occurs in some way. So I suppose I do not find that satisfactory. What was the process of that critical incident being reported to DOTARS and, if that happened, what was their response?

Ms Graham—We report all incidents to DOTARS—

Ms GRIERSON—What is that process?

Ms Graham—It is a written report.

Ms GRIERSON—When an incident occurs, must it be reported within a certain number of days?

Ms Graham—It has to happen, I think, within roughly a day but we would do it straightaway. We would do it mostly by phone, followed up with a written report, and then we would invite them to the debrief.

Ms GRIERSON—Do you know if they came to this one?

Ms Graham—Yes. DOTARS always come to these debriefs.

Ms GRIERSON—Did they make any recommendations?

Ms Graham—I cannot recall without looking at the notes.

Ms GRIERSON—If that did happen, could you let us know what happened and perhaps any response?

Ms Graham—I am quite happy to provide the debrief notes from the meeting. One thing I want to pick up on that was mentioned by the ASU is the issue of a person challenging somebody on the apron who has not got an ID. We spend a lot of time trying to promote a security culture where people do challenge if it appears that somebody is not in the right place. The issue of safety implications for staff in doing so was raised at our most recent security committee. I would have to say that, as the airport operator, we depend a great deal on that sort of culture prevailing, because there just is not enough APS staff on the apron to take on that

accountability. So the whole notion of challenging people is fairly important to our culture, and a number of staff do it.

ACTING CHAIR—Just not this time around.

Ms Graham—I think they did, but they probably did not see him until some time had elapsed. I think the challenge took place.

Ms GRIERSON—You said that you have spent a lot of time trying to develop that culture. How do you do that?

Ms Graham—Through our poster campaigns and newsletters and our induction training. They are the primary methods. We also do it through committees and debrief forums such as I have mentioned.

Ms GRIERSON—Do you have your own security audit process? Do you do your own audit of processes to see whether they are working or not or do you wait for an incident to occur?

Ms Graham—We audit a number of our processes because we know we are going to be audited by the department as well. We are always in a program of self-audit. But there are always issues that come out of debriefs. I do not know how many debriefs I have been involved in over a period of years and there are always recommendations from them. It is a culture of continuous improvement.

Ms GRIERSON—It would be very useful for the committee to see the whole process of that critical incident that occurred—the documentation and the response to it.

Ms Graham—Yes, absolutely. I would be more than happy to do that.

ACTING CHAIR—Do you employ a testing system that has people attempting to breach security at the airport?

Ms Graham—Yes, we do. Usually it comes out of an incident or a DOTARS order. We focus on three key areas. The first, obviously, is the screening point. We also focus on our primary air side access gate for vehicles, which is gate 35. We do tests there to make sure that they do the appropriate checks. We also do those checks through the cargo terminals. One of the weak links to getting unauthorised access is through cargo terminals, so we do tests through those terminals as well—so does the department when it is doing an audit, but we have an ongoing program of conducting those tests. When we see another area of weakness, we look at bringing in another testing regime.

ACTING CHAIR—Do you use that system at all in passenger terminals?

Ms Graham—In terms of screening we do.

ACTING CHAIR—But not in terms of sneaking through a gate when no-one is looking.

Ms Graham—No, we have not.

ACTING CHAIR—Thank you very much, Ms Graham, for coming back and adding to your earlier comments. We appreciate that.

Proceedings suspended from 1.02 p.m. to 2.00 p.m.

GAYNOR, Mr Andrew Garret, Acting Manager, Aviation Policy, Department for Planning and Infrastructure, Western Australia

ACTING CHAIR—I welcome the representative of the state government of Western Australia to today's hearing. We have received a submission from the state government of Western Australia. Do you wish to present any additional material or make a brief opening statement to the committee?

Mr Gaynor—I would like to make a brief opening statement. The submission of the Western Australian government focuses on particularly terms of reference (a) and (e). WA supports aviation security, including at regional airports, and supports DOTARS as the appropriate agency to coordinate aviation security. However, with aviation security, we need to ensure that benchmarking of jet operations is appropriate and fully determine if there is a better option.

We need to acknowledge the disproportionate cost of passenger screening for regional aviation and perhaps a balance needs to be struck between the risk assessment and costs. There is a need to acknowledge further costs of airport security, additional to the cost of providing passenger screening equipment. We make reference in our submission to the case of Newman airport, which has to build a new terminal to house passenger screening.

If I may, I will make a couple of quick observations. Any policy has cost implications, and these need to be carefully considered. It is difficult for regional aviation to bear additional costs. In that respect, we suggest the Commonwealth consider taking some responsibility for costs. Perhaps a source of funding could be any surplus from the Ansett levy, when that is clarified. The state is willing to play its part. Indeed, it has already, through its regional airports development scheme, provided half the cost for the design of the new Newman terminal.

My final point is that these issues have been identified by other state governments. With regard to that, the SCOT—the Standing Committee on Transport—Aviation Working Group is developing a paper for SCOT's consideration of this matter.

ACTING CHAIR—In your submission, you focus on the aspect of who pays for increased security. Can you tell us a little about the position of some of the regional airports in Western Australia? Are they generally owned by councils? What sorts of passenger volumes go through them?

Mr Gaynor—Overwhelmingly, they are owned by local councils, except for Broome airport, which is privately owned. Generally speaking, the figures for regional airports in Western Australia go from Broome, where there are in excess of 150,000 people per year, through to, say, the average size of Geraldton, which has about 55,000 passengers per year. Albany has somewhat less, at around 40,000 passengers, and Newman, which I articulated, has about 40,000 passengers per year. That gives you a spread of the passenger numbers in regional airports within Western Australia.

ACTING CHAIR—You suggest in your submission that any extra costs would be very difficult for the smaller airports to bear.

Mr Gaynor—We believe that the costs of passenger screening can be quite onerous—and I guess in two parts. The first part is the actual cost of providing the technology to passenger screen, but then we have the extenuating circumstances as I have mentioned with Newman where their terminal effectively has to be rebuilt.

ACTING CHAIR—Why?

Mr Gaynor—The airport building is quite small and it just cannot house passenger screening. There are all the other issues which go with passenger screening—fencing and proper design of the terminal. They effectively have to build a new terminal. That cost is in the order of $3 million, by the way. It is quite expensive to build infrastructure of that nature. It is in the Pilbara—a remote location, I guess.

ACTING CHAIR—You have received no offers of help from the Commonwealth government to rebuild the airport?

Mr Gaynor—We have made representations to DOTARS highlighting this issue. To date, we have not had any offers of support. I guess what we are attempting to do through the SCOT Aviation Working Group, which reports into SCOT and ultimately to the Australian Transport Council, is to raise this issue to see if we can have a holistic approach to what is, I guess, when we are talking in respect of Newman's terminal, an extenuating circumstance. I believe there are other instances of this around the country, although I cannot tell you what those are today.

ACTING CHAIR—If, in the smaller airports, the government paid for the equipment and the airports had to bear the cost of staffing the screening equipment, do you think that the cost would then be unreasonable?

Mr Gaynor—I think that is a fair assumption. Ongoing costs of passenger screening is something that perhaps the industry could pay for. If we take out of the equation the particular infrastructure provision—either new terminals or the actual passenger screening equipment—I think that might be the right mix.

Senator WATSON—Does the risk assessment approach pose particular problems for Western Australia?

Mr Gaynor—Let me answer that by referring back to a comment I made in my opening statement about jet operations being the benchmark for passenger screening. We do not wish to challenge that risk assessment. I guess what we are saying is that, if we use the case of Newman airport, which has 40,000 passengers per year, it probably would not have a jet service if it were not for Mount Whaleback Mine. The mining industry underpins that jet service simply on the figures of the people that go to the airport per year. If you compare that to, say, another turbo prop airport like Geraldton airport, which had 56,000 passengers this year, then the question we ask is: is the type of aircraft the appropriate trigger? We are not saying for a moment that Geraldton requires passenger screening because it has higher figures; we are just suggesting that perhaps we need to look closely at the triggers that warrant passenger screening and that it is not necessarily just the type of aircraft.

Senator WATSON—What do you think should be an alternative to the type of aircraft for the purpose of assessment? You say you have problems with that, but what would you replace it with that would make it more viable or have more universal appeal?

Mr Gaynor—It is a difficult question to answer. I do not have answers to that. I guess what we really need to do is work through the parameters of what is required—look at the type of airport and the type of passengers going in there. As I said, Newman has services predominantly based on the mine. There are a range of issues that we believe probably need to be factored in. If, at the end of the day, it comes out that the original assessment was correct, that is fine, but we believe you need to broaden it, apart from just looking at aircraft type.

Senator WATSON—Earlier on we were given an assessment of the costs for some of the minor airports. The figure for a complete upgrading could be of the order of $2 million—$600,000 for the screening plus fencing and other security configurations to the buildings. It would be pretty prohibitive if you were to apply that sort of cost to all the relevant airports around Australia.

Mr Gaynor—Yes, it would be a major cost. Again, I refer back to where we were saying that perhaps a balance needs to be struck between the risk of a situation and the actual cost to those regional airports—bearing in mind, as the Australian Airports Association articulated today, that a lot of these councils that own these airports really do not have a huge rate base to support the cost of maintaining their airport, let alone upgrading significantly their infrastructure for aviation security.

Senator WATSON—An emotional argument is run by people and by newspapers in the smaller areas: why should their lives need to be less secure than those in other places? This has quite a bit of resonance in the local communities, which do not really appreciate the basis of risk assessment or even the impact of the costs which we have been told could close a lot of airports if we went down that track. Would that apply in Western Australia? Would we lose certain airports because of costs or are they too remote and too strategic to close?

Mr Gaynor—Sitting here today representing the Department for Planning and Infrastructure and, in turn, the Western Australian government, it is difficult for me to determine whether airports would or would not close. All I can say on that matter is that there are significant cost burdens and it would put great pressure on a number of airports. But I cannot give you a definitive answer on whether airports would close due to the cost of aviation security.

Senator WATSON—Some airports are in close proximity to other airports. Because of the distances, it has been suggested that, if we go down that route, there would be a lot of rationalisation.

Mr Gaynor—That is not the case in Western Australia. The airports that already have passenger screening, or those which in the future could be on the threshold of having passenger screening should their operations change from turbo props to jets, for whatever reason, are quite widely spaced. Off the top of my head, there would be between 300 and 500 miles between each of those regional airports.

ACTING CHAIR—Doesn't the Western Australian government already subsidise regional air transport?

Mr Gaynor—We do. We have an essential air services program which at this point subsidises four services.

ACTING CHAIR—So there is a possible scenario that, if there were mandatory safety upgrades that airports could not pay for, the burden might fall on the state government?

Mr Gaynor—The essential air services program provides finance to subsidise air services that would not be commercially viable, even for one particular airline. In that respect, there is a social obligation. What you are referring to is the regional airports development scheme, which provides $2 million per year on a fifty-fifty basis with airport owners to provide airport infrastructure. The regional airports development scheme has provided $16 million of state government capital to regional airports and has leveraged in excess of $40 million from the local councils, from the Commonwealth government in some respects, and also from the private sector. Referring again to Newman, we have granted them $175,000 towards the cost of designing that terminal. At this stage the terminal will need to be built in accordance with the regulations. We are now pursuing a collaborative effort with the Commonwealth to look at the extenuating costs of constructing the terminal.

Ms GRIERSON—How is the state government made aware of security incidents at your airports?

Mr Gaynor—I can refer to exactly how the process commences, but I will have to take on notice any specific questions because that relates to another committee, which I am not on. As I understand it, there is a state security unit, comprising local police and others, which looks at those issues. Another committee I report to is the Standing Committee on Transport, Joint Commonwealth-State Transport Security Working Group, which looks at security matters not just for aviation but for maritime and land transport.

Ms GRIERSON—Are these committees of premiers, regional development or—

Mr Gaynor—The Joint Commonwealth-State Transport Security Working Group is a Commonwealth initiative that has state representation on it. There is another officer of the Department for Planning and Infrastructure sitting on that committee and I feed in information relating to aviation security. I cannot comment on specific issues today. I would have to take it on notice.

Ms GRIERSON—So you would not know if Newman has had any specific security incidents?

Mr Gaynor—Not to the best of my knowledge, but I can make inquiries about that.

Ms GRIERSON—I think you have been asked this, but would you suggest that that sort of data and local circumstances should be taken into account in the assessment of the security category for regional airports?

Mr Gaynor—Absolutely. I guess we are saying that, in making that assessment, the criteria used in determining if security is required should be broadened. We are not saying for a moment that security is not required; it is really just broader terms of reference.

Ms GRIERSON—Do you see the time period for implementing these changes as too short or do you think it is realistic?

Mr Gaynor—I believe it is appropriate. Again, I cannot comment fully on that. I would really need to refer that to the other committee, which deals with this on an ongoing basis.

Ms GRIERSON—If the Commonwealth government were to take some of costs—the one you highlighted is a major infrastructure investment and there is very little money for that from the Commonwealth these days; the security equipment itself is very costly—would you make any recommendations regarding the government being a leaseholder of that sort of equipment or taking on that cost rather than each airport having to purchase that equipment?

Mr Gaynor—It is an interesting point. I have not really fully explored the ownership of the equipment. To date, our focus has been that it is an identified cost and we need to really address it in some shape or form.

Ms GRIERSON—If you do come up with any other ways for it to be financed, we would love to know. The other point is that obviously regional airports have very little presence of the Australian Federal Police or the Australian Protective Service and therefore rely on the Western Australia Police Service. Do you have any view on the demands that are placed on the Western Australian police or on the way they interact with regional airports?

Mr Gaynor—I must make apologies—I will have to take that one on notice as well because I am not well placed to make a comment.

Ms GRIERSON—That is fine. Thank you very much.

ACTING CHAIR—We received evidence from the New South Wales government that, because DOTARS do not oversee security measures at uncategorised airports, there is a potential risk with light aircraft or, generally, to small airports. Do you think that that is a significant issue?

Mr Gaynor—A good question—it is a difficult one to answer. I guess we refer to the Commonwealth government, which makes those risk assessments. In the case of our major GA airport, which is Jandakot Airport, they have determined that that is not a major risk, although I would like to add that the owners of Jandakot Airport are being proactive in working with their industry in determining ways of securing that airport, outside the terms of reference. They are working with them to put in more extensive security fencing for their particular businesses down there. So there is some proactive industry work going on there.

ACTING CHAIR—Thank you, Mr Gaynor, for appearing before the committee today. If we have any further questions, may we write to you?

Mr Gaynor—Please do. Would you like me to write back to you about those particular questions that we had?

ACTING CHAIR—Yes, please. Thank you very much. We appreciate you making the long trip over.

[2.20 p.m.]

BECHOR, Mr Udi, Director of International Operations, ICTS Technologies

FOX, Mr Paul, Executive Director, S3 Strategic Security Solutions

LAUDER, Mr Jeffrey Robert, Director of Operations, S3 Strategic Security Solutions

ACTING CHAIR—I welcome representatives of S3 Strategic Security Solutions and ICTS Technologies to today's hearing. Do you gentlemen have a brief opening statement that you would like to make to the committee or any additional written material you wish to present?

Mr Fox—Only a very brief statement. That is basically to say thank you very much for the opportunity to appear in front of the committee. It is a very important process that you are undertaking. We want to pledge our support for the process and offer any help we can give, not just in this hearing but at any subsequent time. The submission that you have in front of you was put forward by S3 Strategic Security Solutions in conjunction with our strategic partner ICTS. Udi is here representing them.

ACTING CHAIR—What does ICTS stand for?

Mr Bechor—International Consultants on Targeted Security.

Mr Fox—Udi has flown to Australia specifically for this hearing. He lives overseas. He has come because of his expertise specifically in this arena—aviation security—not just in the United States but in Europe and Israel.

ACTING CHAIR—Thank you. We might start, if you did not mind, with you, Mr Fox, telling us a little bit about what the company does, and then I am going to ask Mr Bechor to tell us a little bit about his experience overseas. Please start by telling us what your company does.

Mr Fox—Certainly. S3 is a highbred security organisation. It works with a number of strategic partners in Australia and overseas—not exclusively ICTS but ICTS are probably the most relevant and predominant partner we have in relation to this particular issue. We look at high-level security applications in aviation and training of security staff in the counter-terrorism awareness area as well as—as I said—in aviation, major stadiums, government infrastructure and all those sorts of things.

CHAIR—Do you focus on the equipment side, the training side or both?

Mr Fox—S3's mandate is to provide a turnkey solution, hence the relationship we have with our strategic partners, who have particular expertise from a technology point of view. I will not talk about ICTS; I will leave it to Udi to do that. Our aim is to provide a turnkey solution, including project management, technology expertise, audit processes and all those sorts of things.

CHAIR—So you do not build equipment; you advise people what they should be buying in, presumably?

Mr Fox—We deliver solutions for particular needs.

ACTING CHAIR—Mr Bechor, could you tell us a little bit about your experience overseas—what your role is?

Mr Bechor—Certainly. First of all, my title in the company is Director of International Operations. I am also a member of the management team of ICTS International. I have been with the ICTS group for the last 15 years. I serve the company in several countries—mainly Germany. I work very closely with regulators, airport authorities, airlines and others, so I would say security is my real area of expertise. The company, if I may say a few words about it, actually was established 20 years ago and is a consultancy company. Very quickly, the industry and many of the airlines at that time—American carriers—asked us to provide manpower as well and we changed the company structure and started to provide manpower. At the end of 2001 we had about 13,000 employees around the world. Then we sold part of the company for business reasons. During the last 20 years we developed several things that I think have become to be very famous in the industry. One of them was what we called the profile system, introduced at the beginning of the nineties.

Senator WATSON—The profile system?

Mr Bechor—The passenger profile system. It was introduced at the beginning of the nineties. This was after the sad event of Lockerbie in 1988. The American government asked us to participate in that program. We were leading the program and then they adapted one-to-one the ICS profile system and today it is a mandatory system for American carriers.

Furthermore, we developed several technological solutions. One of them is based on the profile system. We call it APS—advanced passenger screening. We understood that a profile was good for a certain time, but profiling caused some problems in the passenger flow. If it took too long and if the passengers did not like it, the airline did not like—even though it is good security. What we did was computerise some of the elements of the profile system, mainly analysing what we call the PNR of the passenger—the personal record of the passenger, their whole booking history et cetera. By analysing that we can have an outcome that enables us later on to speed up the process dramatically—the security procedure of the American carriers. This is, by the way, certified by the FAA. Today it is the TCA.

Later on we developed some programs for training airport employees. Training and audits are one of our main assets for government, airlines, employees, regulators et cetera to use. For example, the last audit we did—a few months ago—was at Schipol airport. It was a two-week audit on behalf of the management at Schipol. We do know how to deal with these things and how to provide all the necessary results and recommendations.

The latest development we have is what we call the IP@SS, a system that integrates several sensors such as a biometric reader—it can be any biometric reader—the APS rule engine I was talking about before and several other elements. The end result is that all the information is stored on a smart card. This smart card is kept by the passenger. That means he carries his details

with him. We do not keep anything in a computer. For the last 1½ years we have been implementing it as a trial in several airports, many in the US and in Europe, and we are very glad to announce that the TSA, Boeing and Lockheed Martin chose ICTS for a pilot of six months with this IP@SS system. That should begin in December and it will last six months. If we succeed, I believe this can be one of the solutions as well.

ACTING CHAIR—What is the advantage of that? Can you bypass security more quickly or get through security more quickly?

Mr Bechor—This is one of the questions that we are always asked. This is also what we try to prove. We moved from the normal manual profile system to this computerised program because we understood that we do not need to look anymore for the negative people. It did not sound good. We did not like that process anymore, so we started to look for the positive.

ACTING CHAIR—Can you explain that? I do not understand.

Mr Bechor—Yes, I can definitely explain it. What I am saying is that, if I take 100 passengers, for instance, who are going to board the next flight, we know from our 20 years of experience that about 95 passengers out of the 100 in one way or another possess a positive sign—that is what we call them—in the reservation and other things. I assume all the people sitting in this room at the moment would be included. About five passengers, and most of the time fewer, out of 100 may cause a threat to the flight. That does not mean they are terrorists; it means that from the booking, the details of the passport reading or from the analysis for security purposes they may be assessed as a threat. Most of the time it is resolved.

We say, 'Let us deal with the five people and not with the 95. Why stop so many people in the process?' Therefore, when we developed this IP@SS system—which we now have in the United States and in Europe—this was our main goal: to really focus on leaving the so-called good people and putting aside not the bad people but those who might cause some problem. That is what the Americans like so much. As we are all aware, with profiling and classification—all of these terms—people do not like to go through them or hear about them. Therefore we changed it in 1997. So we are looking for those guys that we need to take care of. We put most of our effort and energy into those guys—the five guys that I mentioned before, not on the 95—and they pass through very quickly.

In Chicago, where we are going to have our pilot with the TSA being located, we even get a special lane. It is a special lane for those IP@SS card holders for this trial. Here we try to prove the concept that not only will people who go through the system not spend so much time at the front by the check-in check but also they will go in a separate lane with this card—it is an old technological system along the way, but that does not matter—and they will actually arrive at the aircraft on a very fast track by a fast process. So it is not just doing more accurate security and looking for the good guys rather than the bad guys; it is also enabling passengers to pass through very fast. What I am saying is proven, because we have been doing it for 1½ years. As I have said, we have been flattered by the response.

ACTING CHAIR—So do passengers who have one of these cards not go through the same baggage-screening process and metal detectors? What is it that saves time?

Mr Bechor—They do go through, but what happens—and the card looks like this one that I am showing you now—is that all the information is on the card, as I mentioned before. Through the process in the airport we first of all put data for the security process in the check-in, plus a biometric sensor—in this case for two fingers—and from this point of view the information can be read only when the fingers and the card are matched.

Senator WATSON—Only when what?

Mr Bechor—Only when the fingers—the biometrics here—and it can be a fingerprint or it can be any sensor or it can be voice or it can be a physical matter—

Senator WATSON—That was the weakness they had with the card because if it got lost or stolen somebody could manipulate it.

Mr Bechor—I have two answers for that. We are not producing the card. We chose the card after long research. We believe that this card is one of the best cards that you can find today in terms of breaking in and taking the information out. Furthermore, if I can use the term of a key and lock, the fingers are the key and the card is the lock and only when they match will it open and you can read information. So in the process, after the passenger has left the check-in and goes to the baggage check and to the other matters that you have mentioned, he then puts the card again on the reader with his fingers. The security personnel will see the certification—and I use the term 'certification' because I do not know a better word—from the check-in and if a person is a selected passenger he will go to one side and if a person is non-selected he will go to the other side, but both will be checked. The only difference is that the selectee will be checked in a different way. So we expedite the process for the non-selectee, as I mentioned at the beginning, and we have all of this information also at the gate before they board the aircraft. In America selectees will be pulled aside in some airports and the rest will just proceed to the aircraft in a faster and quicker way.

Mr Fox—The advantage of that is that you are focusing all of your screening resources on where they are most likely to have the best result. So you are focusing on the people who are already determined to be much more likely to be a threat, rather than screening everybody.

CHAIR—This works if you are a frequent flyer. If you are flying all the time, I can see its advantage as a fast-tracking system. But most Australians would not fly at all or only once or twice a year, so you are not going to present them with cards, are you?

Mr Bechor—I do not know when the people in the room travelled last time to the States, but I can tell you that even if you travel only once—I travel a little bit more than once—it is better. I see all those passengers who travel only once standing there sometimes at certain airports with a one or 1½ hour wait for a security check—those with kids or those who are elderly people—and nobody likes it. Going back to what you said about frequent travellers, I agree 100 per cent. It is beneficial for frequent travellers.

Now we have presented to the American government—and this will be tested in a trial that starts in December—what they call the trusted passenger program. That means that the government will be able to make a background check on passengers who will voluntarily apply for these cards. We will never have the data of the government—we do not want it and it is none

of our business—but we will get the outcome, which may be, 'Okay, Mr Bechor is entitled to get the card.' I will then go through the enrolment the first time at the airport and get the card, but the card will not help me if, when I come to take the next flight, the rule engine shows that there is a problem with my itinerary, PNR or other signs. So it is a benefit, but it is not a joker card, if I can use that term. It does not mean that, once you have it, you can go and pass through and nobody will check you. You will always go through the enrolment in the airport, but the enrolment will be short and you will probably not feel anything.

Ms GRIERSON—If I wanted a card, who would I apply to—Continental Airlines or to IP@SS?

Mr Bechor—At the moment, because it is a Continental Airlines-ICTS card, you will not apply; you will receive it at the check-in while you go through the security process.

Ms GRIERSON—So what information does it have on me?

ACTING CHAIR—So you do not carry it with you all the time, it does not belong to you; it is handed to you at check-in?

Mr Bechor—I will explain it again.

Mr Fox—Only at the beginning when you first get it. Once you are given it, you will retain it.

Mr Bechor—Once we give it to you, it is yours.

Ms GRIERSON—What information is on it?

Mr Bechor—We captured the photo and the first data page from the passport, the positive code, if you have one, from the APS system and all the components of the government watch lists. In America we get all the FBI listings et cetera—stolen passport lists and many other things which we check against. Everything will be stored here and, in this case for this moment, it will be your security card—plus the classification.

Ms GRIERSON—Who owns that information?

Mr Bechor—In general, the PNR will belong to the airlines.

Ms GRIERSON—So can you sell that information to someone else?

Mr Bechor—No. Again, the PNR itself—the information that we analyse for security purposes—will belong to the airline and will stay with the airline. We only analyse it; the information is not collected by us.

Ms GRIERSON—So, if the airline owns it, could they make it available to their associated travel agents or whatever?

Mr Bechor—I am not here to answer for the airline but, knowing the business, they never sell it. This is the airline's most restricted information for commercial reasons. They do not want to

let anybody get it, because of the frequent traveller status and other data about their premium passengers. Again, I do not represent them but, knowing the airlines, this is something they keep very close to the chest.

Mr Fox—I am not sure whether we have explained what you can tell from the PNR record. There was a screening issue—you can tell things that identify that person as a possible threat, like who paid for the tickets and so forth. Would you explain that?

Mr Bechor—With your permission, and it should be confidential—

Senator WATSON—We have press here.

ACTING CHAIR—Are there any journalists here? If you say something now, it will be recorded in *Hansard*, so it is possible that journalists or the public will have access to it.

Mr Bechor—I do not mind sharing with you the rules but, with your permission, I would like to send it to you. I do not want to make it public.

ACTING CHAIR—There are two ways we can do it. You can just send us the information and mark it 'Confidential' and it will be treated as confidential. The other thing we can do is to stop for a moment and ask all of the people who are not committee members to leave the room and we can hear your evidence in camera. Which would you prefer?

Mr Bechor—It depends on you. If you would like to hear it now, okay; if not, I will submit it to you in writing. I can talk about the concept.

ACTING CHAIR—I think it is better if you send the information in writing marked 'Confidential' and just talk to us now in broad terms.

Mr Fox—I think it is important that you have some concept of this, because it is probably important to the understanding of the rest of it.

Mr Bechor—In general, by analysing the PNR, there is a lot of data about the way you make the reservation and about who initiated the trip, flight and other information that can be relevant for security purposes. I will compare it. If I take a flight ticket now—and this used to be the old system of the profile—I read the flight ticket and I analyse the data from the flight ticket and compare it to what we call a 'suspicious signs list'. Today the computer is doing it. Today you find those signs that we can find on the ticket. Because we dig into the PNR that the airlines send us, we have more information than usually appears on a ticket. The rest, I will be very glad to send you.

ACTING CHAIR—I am even guessing that it would be things like paying for the ticket in cash and signs like that.

Mr Bechor—I am not going to answer.

ACTING CHAIR—Okay.

Mr Lauder—The 9-11 incident is an example of how those tickets were booked?

Mr Fox—Is that confidential?

ACTING CHAIR—No, that was in the newspapers.

Mr Bechor—No, it is not, but I do not want to relate it to our system, because otherwise I will be in trouble with the Americans.

ACTING CHAIR—Okay, thank you, but we would appreciate it if you could send us the additional information for our confidential treatment.

Mr Bechor—No problem.

ACTING CHAIR—You carry this information with you and it fast-tracks you through an airport. How much background checking of people can you do? How much information do you have access to? You say you have access to FBI watch lists.

Mr Bechor—Not exactly. I will elaborate because it is a very important thing that I will make clear. First of all we do not have any access to any governmental data. I am not plugged into anywhere where I can take data away, except for the PNR, which is commercial information that every airline has and it is beneficial for security. I get from the FBI through the airline every second or third day an update of what they call the watch list. I download this to the computer and when we compare the name from the passport with the names on the watch list I can make a match. I am not online or in any other way plugged into the FBI computer. I do not want to and it is not our intention. I am using the list an airline usually gets in soft copy. We get it straight forward to our computer and we analyse those lists. It is the same with stolen passports: we get the list from the government. It is not that we are online or something with the data of the government.

Senator WATSON—So in America you might have six cards for six airlines?

Mr Bechor—I would be very happy if we would have it.

Senator WATSON—If I fly frequently out of a place like New York, I might have six airline cards; is that right?

Mr Bechor—It is again an excellent question. While we have dealt with several airlines up to now with this concept, we say: 'Guys, maybe one day you will sit in one room and decide that it will be one card.'

Senator WATSON—At the moment it is six cards.

Mr Bechor—At the moment it would be six.

Mr Fox—That is also the opportunity we are looking for. Australia is in a unique position where it can start from the beginning. We can decide on the system that would possibly be the system across the board.

ACTING CHAIR—Mr Bechor pointed out a good issue before. Anyone who has flown into or out of the United States recently will tell you that the delays at US airports are substantial—and I think that that is true of a lot of countries—but that is not really true of Australia at the moment. Our security processing is pretty fast in my experience.

Mr Fox—I am perhaps not qualified to comment on that. Perhaps the airlines would comment on that. We are not so concerned about how long it takes to get through; our comments are aimed more at how to enhance the level of security. We are asking if we can potentially devote more resources to where they are needed most, because at the moment we are screening everybody to the same level, pretty much.

ACTING CHAIR—Could you combine the information that you have on this card with your airline frequent flyer card and have a seamless system where you could have automatic check-in, put your frequent flyer card in, get your boarding pass and fast-track through security with this card with the biometric reading? Could you have all of the information essentially recorded on one card instead of carrying a number of them?

Mr Bechor—Yes. Actually you touch on the next development of ICTS and—if you allow me no names of commercial companies—one of the major US companies that produce what they call a kiosk. In America they have a kiosk, and that is what you have just described. That means that a passenger today has access to kiosks, mainly for domestic flights. The next development that ICTS is involved in with one of the major suppliers is to have kiosks for international flights as well and also to provide security up to a certain extent for the domestic flights. One person at least always needs to stay near those kiosks in order to watch for what we call the appearance of nervous signs.

All the process would be done by the passenger without anybody standing in front of him. Yes, certainly it can be connected as well to the credit card and to the frequent traveller card. Some airlines when they talk about the kiosk ask us to put on an electronic wallet so people can buy in the airport with this card and more and more commercial things. We are working on the kiosk. It is something that the American government is very much interested in as well in order to expedite the process. I think we have a very good solution for that. I hope we can show something to the market soon, but we are in the process already, yes.

ACTING CHAIR—Doesn't that raise issues of hold baggage screening? If you are checking yourself in, particularly for international flights, who is checking your bags?

Mr Bechor—Where—America?

ACTING CHAIR—You are saying that some people are interested in extending this to international flights.

Mr Bechor—I am not here to represent the American government, but the concept today in the States is that you could even leave your bag with the security people for this HBS. In most American airports it is done near the check-in. You go there and they ask you to unlock your bag. Then a person from TSA will take the bag and 'X-ray it'. It is not exactly X-ray; it is a bit more sophisticated. The same can happen with the kiosk. You finish with the kiosk and you get a tag for the flight. The person there will assist you—if you need an assistant—with the tag. Then

either you take it and you wait with your bag or you just take it and bring it to the same position that you would through the normal check-in.

Furthermore, more information could be put on the baggage tag et cetera, so the people who X-ray your bag will get some information about your classification. So there is a very large scale of possibilities here. But we will only present it to the market when we are sure that all the loopholes are closed. That means that nobody can cheat the system if you go to a kiosk. We believe we are there, but the government—in the case of America, the regulator—needs to approve it. I think we can close all of these loopholes where somebody on the way could play with your bag or do other things.

ACTING CHAIR—If you get your boarding pass and you are about to put your bag on the conveyor belt, you can imagine 20, 30 or 40 people checking in in a queue. With one person supervising the kiosk, it could not be that hard to slip something extra into your bag.

Mr Bechor—Firstly, I did not say 'one person'. I said there would be at least one person near the machines. I was not talking about quantity; more about quality. This will be part of the concept as well. If we have, let us say, 10 kiosks—I assume it will not be one person; there will be more—our concept, like the many technological developments that the company brings to the world, is always that somebody, a person, needs to be near this equipment. I do not see ICTS selling any technological solution, or any solution, without a human being being there and monitoring the process, mainly to check the appearance of people and be ever suspicious. That is a very important factor in detecting a threat to flights.

ACTING CHAIR—You mentioned earlier that you started your career in Israel.

Mr Bechor—I was born in Israel.

ACTING CHAIR—Did you work in the airport at Tel Aviv?

Mr Bechor—No. I served in the military, unfortunately—like everybody else in Israel.

ACTING CHAIR—I was just wondering because the security at Tel Aviv is extremely high. You do not have any incidents there.

Mr Bechor—Extremely high, yes. I did not serve there. I went abroad and did some other jobs and then I joined ICTS.

Senator WATSON—Privacy issues are fairly strong in Australia. Have you encountered that elsewhere?

Mr Bechor—Yes. I did not finish my answer to Ms Grierson's question about the data. I will elaborate. Everything will be stored here on the card, and it belongs to the passenger. From the moment he gets it, it belongs to him. We will not keep any information. We delete all the information after the flight. The only thing we will not delete is the APS code. This is because the regulators—in this case the American regulator and the Dutch regulator in Holland—asked us to keep it for at least 24 hours in case, God forbid, a plane crashes or any sabotage occurs. So we keep the data in the computer only about the classifications of the positive code for at least

24 hours. Later on it will get decoded for, I think, three or four weeks, so nobody can read it. Again, if there is an investigation because something happens, and the government, the regulator, would like to investigate, we can encode it. After 30 days, I think, it will get automatically deleted. All the rest of the information is here, not in our computer.

Ms GRIERSON—So, if I want to read my card, some sort of scanner is used to read it. Does that mean any scanner can read it, or are they matched?

Mr Bechor—No, it must match. It is not a scanner; it is a card reader. The card reader—and I might be using a basic explanation—must talk to the card. If it does not talk to the card and it is not in the same algorithm, you cannot access the information.

Ms GRIERSON—If eight airline companies are offering smart cards, aren't they going to want, for ease of getting all those people through, a common reader?

Mr Bechor—You mean if different airlines participate in the same program? They may, and then we would need to develop the right algorithm for it. I think it is possible but, again, we would need to pay attention so that it would not be influenced by other people. I am not sure that this would be the end product. I think the end product would look different. I think the American regulator, after the tests in Chicago with Boeing and with Lockheed, will choose ICTS to be part of the solution. I am saying clearly that ICTS is too small—with all respect to ICTS—to implement the solution in 429 airports in the US. We have no such business plan or any intention to do so. Therefore, those entities agreed that we would be part of it so that they can implement it. Then, as I see it, there would be one reader for the regulator, not for the airline. The card would be issued by the regulator; then one reader would be okay. It would be for every airline—it would not be commercial.

Ms GRIERSON—So you can see Customs or Immigration having common access?

Mr Bechor—Yes, whoever—an official entity. This would be a part of the trusted traveller program—or whatever they call it—and they would issue the card. Back to the privacy issue, when we developed this APS engine to deal with the PNR et cetera, we went through a very long process with the Dutch government, who in those days hosted this project with KLM, and we received approval from the Dutch government saying that the privacy issue was more than good, it was perfect, and there were no problems. This is applicable, by the way, to all the EC countries. Furthermore, the American carrier gave permission to have and use this data, knowing that privacy was maintained at all time without any problems. We can submit those papers if they are needed.

Senator WATSON—If you are a farmer and have rough hands, with cuts, bruises and scratches, does that affect the reading ability of a card?

Mr Bechor—Yes, it can affect it. But you would then go through the usual process. I would hope the airline and security people would handle you the same as they handle those passengers, but you would go through the usual process. There are always exceptions. If somebody does not have their right hand or both hands—it can happen—and the reader will not read or whatever, then you would go through the normal system. Unfortunately, it would take a little bit longer.

Mr Fox—It may not be finger reading either. That just happens to be the chosen biometric device.

Mr Bechor—It could be any place.

ACTING CHAIR—We do not like eyeball reading, because we have all seen that terrible Arnold Schwarzenegger film.

Mr Bechor—In some places where iris readers are installed people ask the operator, 'Can you give me a report for my drivers licence that my eyes are okay?' Any sensor that the government choses we will implement.

ACTING CHAIR—Mr Fox, you said earlier that this was an advance on ordinary passenger profiling. We do not know much about passenger profiling in this country. Can you tell us a little bit more about it?

Mr Fox—I will defer to Mr Bechor again.

Mr Bechor—I came such a long way from Israel, so it is good I am getting to speak. If I understand your question correctly, I think profiling is something that we all do often. We profile people when we enter a room and look around. Profiling is a very broad term, but when we talk about security we try not to use the word 'profile'. As I said before, we are looking for a minority—a small group of people who may cause a threat to a flight. I do not think the rest of the people—the majority—need to go through the same process. I think, even in Australia—and I do not know Australia so well, but I am trying to follow your question—if the government or the regulator were to adopt a system similar to this, from ICTS or any other company, then you would look for the positives in the reservation and other things that the passenger shows you. I believe that would be easier than if we talk about profiling people, which would lead to discrimination issues et cetera. I hope I have answered your question. I really believe that the word 'profile' should be put aside. We should look for those people who can threaten the flight, but all the others should pass quickly.

Mr Fox—Can I just add to that answer. Certainly on our travels we have come across this issue several times in talking to different airlines, regulators and so forth. The issue of trying to find the bad people rather than just trying to find the bad items—the things they are going to use to hijack the aircraft—has to be considered in conjunction with what is already being done. Looking for the knives, guns, bombs and things should not be dispensed with but added to, to try and focus the attention where it is needed, because we do not have unlimited resources. Certainly in Australia, with our population and so forth, resources are an issue as far as providing the security is concerned. As Udi said, eliminating the majority who are not going to pose a threat is very easy to do and then attention is focused, fairly heavily, on the people who statistically are going to present more of a threat.

ACTING CHAIR—How much does a system like this cost?

Mr Bechor—I cannot answer—not because I do not want to answer. It depends on so many factors. If it were one system to one airport—one machine and that is it—

ACTING CHAIR—What if you had one national system that applied in the major airports in Australia—say three or four major airports?

Mr Bechor—I am not running away from the question. It is really hard for me to answer. There is a configuration of the 'machine'—I am calling it a machine—which is about one cubic metre. It is more expensive. There is a very small unit you can implement on the check-in desk so the passenger only sees a small screen, where we use the computer of the airline with a different file that the airline employee cannot open. There is a mobile unit. There are so many varieties—and I do not mind submitting you a price for each one of them—but it really depends in the end on what the client wants: in this case, on what the Australian government wants.

I think, first of all, we need to study a little bit together. I think we would make a study first about the flow and about the problems. Do business and first class always check in separately? Maybe you can start there and put only a few machines in there. Would you like to have mobile machines, because you have different check-ins and you need to move from one check-in to the other? Is it always a permanent check-in for those flights that you want to check? Would you like to implement it in the central checkpoint as well, as we are going to do in Chicago, or do you not want to put it there? Are you going to implement one in the gate—yes or no? All of these questions are, at the end of the day, what we need to know in order to give you a price.

Mr Fox—Can I comment on that as well. I think the overarching issue here, though, is that it is about providing a high level of security in a very cost-effective way, because you are utilising some very innovative technology. At the moment, one of the solutions being suggested is more manpower—more security staff. That may be a part of the solution—I am not saying it is not—but if we can provide a much greater level of security with fewer people—not fewer than we currently have; no one is suggesting that—that is probably going to make the whole system much cheaper. It is about working smarter rather than just harder.

Ms GRIERSON—Have you given presentations to the federal government in regard to these security systems?

Mr Fox—Yes. We have been in various stages of dialogue with the airlines, the airports and the regulators.

Ms GRIERSON—In America, is the take-up for easing the flow of domestic rather than international passengers?

Mr Fox—Correct.

Mr Bechor—Out of the few hundred million passengers a year in the US, about 85 per cent are domestic. So they are more interested in a solution for domestic passengers.

Mr Fox—It was also domestic aircraft that were used in September 11.

Ms GRIERSON—How do you acquire 100 points?

Mr Fox—The suggestion we made in the submission was a hypothetical suggestion, in the sense that we are probably not in a position to put forward an answer for how we classify or

identify people as that is a government issue. However, we are saying, in its simplest terms, that you have to present 100 points to open a bank account so could that apply here. There are still some problems with that, but that was there as a thought-provoking suggestion.

Ms GRIERSON—I probably differ with the acting chair's comment about regular travel. I tend to find that I am travelling with the same people on the same planes all the time. From a regional city, people fly to work all the time, whether it is to Melbourne, Brisbane et cetera. So there is great frustration at times when you are going to the same airport, you are the same person and you have to pull out your photo ID et cetera each time.

Mr Fox—My suggestion there is that, even if 10 per cent or 20 per cent of the passengers who fly regularly are subjected to this new process, it is going to take a workload off the existing screening and security system. A national system is possibly a first place to start. We are lucky that we are in a position to be able address that issue at this point, but there are some shorter-term options for us and that would actually make a difference already.

Ms GRIERSON—There are some who would say, 'Why do I have to go through it?' and that is really not what you want to happen.

Mr Bechor—Mr Fox has elaborated on the 100-point system, but I think one of the problems in Australia—and I call it a problem from the committee's point of view—when dealing with domestic passengers would be the fact that you do not always use a drivers licence, as I understand it, and you do not have an ID. The system somehow needs to deal with a person standing there with a document and the official knowing whether or not this document is the right document.

ACTING CHAIR—You can use your lounge card or your frequent flyer pass, not necessarily a photo ID.

Mr Bechor—We can find a solution, but the point is that it is really hard in Australia. It is not a problem internationally: you present your passport and from that moment the process starts. We can find a solution for Australia if you ask us to, but I think this 100-point system could be just one of the ideas.

Ms GRIERSON—Have you had an opportunity to test the security of your smart cards?

Mr Bechor—Do you mean that nobody can break the encryption? Yes, we do it very well. It is not only that we do it very well; the TSA have asked us to provide a six-month pilot in Chicago—and we are going to start next month—and this was one of the main issues. I believe that during this six-month pilot they will use hammers, screwdrivers—anything—to try to break it.

Senator WATSON—From your experience, what do you perceive to be the weakness in Australian aviation security at the present time? You have had a lot of experience around the world.

Mr Bechor—It would be unprofessional of me to give any answer on that because I do not know. I can talk in general, but not about Australia.

Senator WATSON—What about Mr Fox. Can you perceive weaknesses in our system?

Mr Fox—If I could be so bold as to put forward a personal opinion, there are a couple of deficiencies. One is the lack of passenger screening, having access to data that is already available and to the advanced passenger screening. Issues such as who paid for the ticket, when it was paid for and any changes that are made—all those sorts of things—are being used in other countries to identify whether this person has a 'flag' as far as them being a possible risk. So there is the lack of that screening in processing passengers. The regional airports issue is still a major issue. It is being able to deal with the number of passengers that need to be screened with the limited resources.

Mr Bechor—I want to add one thing—and I want to speak in general because I do not know about Australia in particular. I can assume that maybe I know something, but I do not like to assume. In general, I think that the first problem is: do you have a threat? Does the Australian government think there is a threat to Australian aviation? I am asking that question not in order to get an answer now.

I think this is the point where it should start. Once the government and the regulator identify the threat, from my experience, I believe the next level is to start to deal with the threat. Is the threat just for international flights? Is it just for domestic or is it for both? Is it for every airport or for particular airports? I can give a variety of questions that need to be answered in this case. Then I think people like us in this case can bring their expertise into such a working group or such an environment, dealing piece by piece with this threat and seeing what the right solution will be. What is done today, and what can be the solution of tomorrow, may only be training and supervision, and maybe an audit system will be enough. Maybe it is technology. Why should you spend so much money on technology when it is not needed? I think it would be unfair to talk about either the lack of security on the whole. On the other side, when the government define the threat, from this point we are placed, if it is us, to start to give answers. But some governments, even if they think they have a threat, later on say, 'We do not think that we need to increase security because everything is okay.' There are governments who speak like that as well.

Senator WATSON—Do you advise security intelligence agencies of countries on security?

Mr Bechor—No.

Senator WATSON—It is just a commercial operation.

Mr Bechor—Yes.

Mr Fox—Can I add to my previous answer. I think one of the other issues is that the security-screening process that is being undertaken at the moment in our system is treating everybody the same. We are processing every single person who is not just flying but seeing their parents off or greeting friends, family or whatever. We are potentially putting more people through the screening process than we need to. It is the people who are getting on board the planes that are of more interest to us. I think that perhaps some radical thinking is required to look at the existing system. I am not suggesting that I have all the answers here, but one of the things we mentioned in our submission—and it may put the cat amongst the pigeons in the industry—is perhaps changing the structure of the airports whereby only the people who are flying go through the

intense screening process. That would actually consolidate the resources that we have to where they need it the most.

Mr Bechor—One of the problems is that governments sometimes invest so much money, and they think that they can now go to sleep in peace and quiet, but the procedure is not kept on the field. The supervision is not done correctly. There is no audit and quality assurance system.

ACTING CHAIR—As we found out today.

Mr Bechor—You put in so much money that, at the end, it is not beneficial. I really believe in the full concept. The full concept is from recruitment to training, supervision, audit and technology solutions. But first of all is the definition by the government if there is a threat or will be a threat.

ACTING CHAIR—One of the issues that a number of our witnesses have brought up is that, with the outsourcing of security-screening functions, you get a lot of causal staff, the training is uncertain and they are not working regularly on screening machines, which are reasonably complicated equipment to read properly. From your business perspective, do you have any view on that?

Mr Fox—I might defer that to Udi as well. ICTS do provide training for X-ray operators throughout the United States and in Europe. That is his expertise.

Mr Bechor—We do. Due to the fact that we also have manpower in certain airports around the world—and I must respect our competitors because they also provide manpower—I know that when you have manpower you also have mistakes and problems, even ICTS. That means that, within the teams, not everybody is always perfect. With your permission, I will speak in general in order not to touch on any of the manpower companies. Again, if you follow what I have just said about recruitment—and ICTS is doing it—you should set a real guideline for the recruitment. Who is a person that should work as a security officer or agent—whatever it is called—in an airport? Sometimes we choose people that we think can do it with no problems. They make a great impression, but they are very bad in passenger service—and we should not forget the passenger service. Sometimes we have great people in passenger service who cannot operate a machine for a variety of reasons. Sometimes you employ people who are colourblind and you need to analyse the colours on the screen. Some entities are not paying attention to it. We are talking about very small things that are very important sometimes.

Furthermore, I think that we have a good training program—and again I can only speak for ICTS in this case—and I know that it has been accepted by several governments and by a lot of airlines; otherwise, they would not work with us. I believe that training is the first real stage of introducing security to the person in the way that they are going to work later. Here you need to pay a lot of attention to what you are telling them, what you are showing them and how you teach them. We have computer based training and frontal training. We have a lot of variety. All systems need to be clear to them when they go to the field and start the OJT—the on-the-job training—and later on when they apply for certification.

This certification needs to be something that the employees are working towards, instead of thinking, 'I will get the certification anyway.' It needs to be regulated and there needs to be a

standard. In this case, for Australia, there must be one standard. It sounds as if it might be a dream, and I hope I am not naive. I think that even in a country as large as Australia you can set standards. You should have standards. There is no way that an airport with two flights a day should have different standards from an airport with 500 flights a day.

You keep the standards up through ongoing trading, supervision—as I mentioned before—and auditing. In the end you might need to fine the company, the airline or whoever and then they will know that it is serious. Sometimes with an audit system, the auditor comes, they go and nothing happens. We are dealing with human beings. Some of them think, 'Nothing happened, so let's continue.' It is like a kid whose parents are coming home, and they do not care if they make a mess. Some people misuse it. We believe in a full concept, as I said, so that real security can be provided.

Senator WATSON—These people with all this high training would be fairly well remunerated. We tend to remunerate them at the bottom end of the scale.

Mr Bechor—I do not understand.

Senator WATSON—Where do these people fit in?

CHAIR—Should they be paid more if they get better training?

Mr Bechor—You are the one who pays, so I would never say yes, but—

Mr Fox—We are not here to suggest whether those rates of pay are right or wrong, but I think some attention can be applied to the training and the regulatory audit process of it. As Mr Bechor said, it is about having some consequences. My opinion is that in the past perhaps we have not paid enough attention to the important role those people play. Not only have we not paid attention to that but we have put them under extreme pressure. We obviously pay a lot of attention to this part of our travel because of the industry we are in. Those operators are under a lot of pressure socially. They are often abused and they are not paid a lot of money. They are doing the best they can, but they are probably not being trained well enough in the first place. One of S3's primary projects in the next 12 months is to develop an academy for security training and counter-terrorism awareness in Australia. We are in the process of making representations to state and federal governments in relation to setting that academy up. It could address issues like that to increase the standard.

Mr Bechor—Without touching on the money issue, I think that one of the problems is—and we all fly; I am sure some of us quite a lot—that when I fly I am putting my life in the hands of somebody who needs to take care of my security. He should not make even the smallest mistake. When we talk about September 11, the weapon we are talking about is a cutter. With this cutter, 19 devils—allow me to call them that—succeeded in using an aircraft as a rocket against a building. It was a small knife, not a pistol, a rifle or a bomb. That is what these guys used. They entered the cockpit, manoeuvred the aircraft into a building and killed 3,000 people in New York. We are talking about a simple modus operandi of a terrorist, but because maybe the regulator did not ask to look in their baggage, or maybe because somebody missed the knives, they succeeded in doing what they did.

As a passenger, when I am sitting 30,000 feet above the ground, I am always—even if they work for ICTS; it does not matter who they work for—wondering, 'Did they do the best work they could?' We are dealing with somebody who is taking care of our lives. When we go to surgery or to a doctor, we check 10 times before we lie on the bed and let them perform surgery on us. At an airport, you might go through security every day. These people may some day cause your death. Do we take care of these people, the procedure, the recruitment and the payment? I do not want touch on the point of payment, as I said before.

Sometimes they bother us. We think: 'What? You are opening my bag again?' But when I am sitting there I hope that they open every bag and I hope that they know what they are doing when I fly in order that I can see my daughter and my wife again. I am serious. Sometimes we handle these people like pizza service people. I think this is a problem. If a passenger sees that everything is in hand, if they see technology and they see seriousness, I am sure in the long run they will appreciate it, because it could mean their life. We are talking about our lives. We are sitting in these aircraft.

ACTING CHAIR—I would like to thank you for appearing before the committee today. If we have any additional questions, I ask that we be allowed to write to you and ask for responses in that way. If you are able to send us the information that you mentioned earlier, we would appreciate that as well.

Mr Fox—Can I just make a short closing statement.

ACTING CHAIR—Yes.

Mr Fox—I just want to offer our assistance, if required, in a fairly intense way. Obviously, we live in Australia, we have a vested interest in aviation security from a personal point of view, and we want not only to offer our support within the context of our professional outcomes but also to lend any assistance that we can and open up access to anything that we have available through our network.

ACTING CHAIR—Thank you, Mr Fox—and especially for making such a long trip to address the committee today.

Mr Bechor—It has been a long and, up until now, a safe one.

[3.17 p.m.]

MAOR, Mr Moshe, Managing Director, ToLife Technologies Pty Ltd

MEITAL, Mr Moti, Senior Security Consultant, ToLife Technologies Pty Ltd

ACTING CHAIR—We welcome the representatives from ToLife Technologies to today's hearing. Gentlemen, do you have an opening statement that you would like to make or any additional material that you wish to present to the committee?

Mr Maor—I would appreciate the opportunity to make an opening statement as well as to table these documents.

ACTING CHAIR—Thank you.

Mr Maor—Until September 2001 the world aviation industry neglected to invest in protection. However, since then it has become the major issue in world aviation. In 2002 a strategic partnership between an Australian company, ToLife Technologies, and two Israeli companies—Pro-Tact and ELTA Systems, which specialise in the homeland security field—created the ground for a partnership which provides a global solution for homeland security at a national and regional level. The comprehensive national level solution for aviation security provided by our companies is based on existing capabilities such as an aviation security system in airports and passenger aircraft protection. The company continues to expand its client base globally in the field of aviation security and protection. Its successful track record in the Israeli aviation industry—as well as in projects in conjunction with the US government—illustrates the company's ability to leverage its know-how and to plan, develop and create a cost-effective comprehensive security solution for the Australian aviation industry.

After the hijacking of an El Al flight to Algeria in 1968, the Israeli government decided to put the responsibility of aviation security in the hands of the Israeli Security Agency, which is better known as the Shin Beth. The year before September 11 changed the way many countries would think about aviation security. Israel was already a pioneer and world leader in aviation security. My partner, Mr Meital, is a senior security consultant and director in ToLife Technologies, whose expertise is based on the fact that he was a director in the Israeli Security Agency. Among many of his responsibilities for security roles within Israel, he was the director of security in charge of all Israeli civil aviation, passengers and cargo security in Israel and overseas between 1998 and 2002.

ACTING CHAIR—Thank you. My own experience going through Tel Aviv airport is that a great deal of the security is not based on any sophisticated technology but on personal searches and even on stopping vehicles before they enter the vicinity of the airport and doing basic checks then. How much emphasis would you say you place on the technology side of security compared with the human side of security?

Mr Meital—I would say fifty-fifty, because we believe that aviation security and security at all is some kind of combination between technology and the expertise of human beings. We base

our expertise on the human being. We find it very important even today. Of course, what you saw in Tel Aviv is not the optimum situation. Israelis hope that in 2004 we will open the new terminal and there will be more technology. The problem is that in the current terminal there is no space for that technology; it is too small. That is the only reason we do not use more technology.

ACTING CHAIR—What sort of technology will you be relying on in the new terminal?

Mr Meital—It is based on three levels—X-ray machines, CT machines, sniffers et cetera. It depends on the level of threat from the passengers. The gentleman from ICTS talked about classification or something like that. We believe in classification. There will be passengers who will be treated with three levels of technology—the basic X-ray machine, then the CT and then the sniffers.

ACTING CHAIR—Do you use trace technology? In Australia we have just introduced a system where the baggage is swabbed and checked microscopically for particles of explosives et cetera.

Mr Meital—We plan to use it in the new terminal.

ACTING CHAIR—Will that apply to 100 per cent of baggage?

Mr Meital—Yes, 100 per cent baggage screening.

ACTING CHAIR—Do you X-ray all luggage going into the hold of aircraft?

Mr Meital—Today? No.

ACTING CHAIR—Today it is searched physically, though, isn't it? Today you take your bag—

Mr Meital—Yes, we classify the passengers according to terrorist profile and we decide who to check and who does not need to be checked. But on the gate all the passengers are checked.

ACTING CHAIR—In your submission you talk about a comprehensive integrated security response comprising advanced technology, command and control systems, security deployment and security screening procedures. Would you describe this sort of integrated system to us?

Mr Meital—It begins with the recruitment of the people to fix standards such who is going to be a security officer. It continues with the risk analysis, the formulation of security plans, advising you which kind of technology to use and what are the vulnerabilities and threats—a comprehensive solution for cargo, passengers, luggage, catering and everything that comes to the airport.

ACTING CHAIR—Your security system includes comprehensive responses to such attacks as missiles, anti-aircraft fire, car bombs and powerful explosives. These weapons have never been used against Australian aviation. Do you think it possible that they will be used in Australia or do you think that relying on such a system would be overreacting in our environment?

Mr Meital—We Israelis have had very bad experiences—I am sure you have heard about the attack against the Israeli flight in Mombasa—so we are going to use it. We do not use it now because it is not certificated by the FAA. But I was updated before I left Israel that it is going to be certificated in six months for use on commercial flights. It works; it is approved technology. We have put it on presidential planes all over the world. They are not commercial planes. They are like US Air Force No. 1.

Senator WATSON—Do you perceive any strategic weaknesses in the way we go about security in Australia?

Mr Meital—At this stage it would be superficial to answer you. I came yesterday, at midnight, to Australia. This is my first visit. I could not give you a serious answer.

Mr Maor—I believe a risk assessment needs to be done properly. A study needs to be done, which we have not conducted. So any answer would be just too shallow and not satisfactory.

Senator WATSON—Would you like to comment on any of the evidence given by witnesses today? From your background and your experience, have you any observations to make on what has been said today that could assist the committee?

Mr Meital—I know that in Australia you base all the security at the airport on technology, and I think that is not enough. As I said before, it is a combination of human expertise and technology. You have put everything on technology.

Senator WATSON—And you think that is a weakness?

Mr Meital—Yes, I think it is a weakness.

ACTING CHAIR—Do you think our weakness is in the recruitment process, the training process or the conditions of the work?

Mr Meital—From what I have read, I know that there is a huge difference between the international airports and the domestic or regional airports. It cannot go like this. There is no need to make any difference between airports. The threat is the same threat. You have to use the same standard, the same system, the same technology, the same concept, the same culture and the same atmosphere. This is security. A plane that takes off from a regional airport can make the same damage as the plane that takes off from an international airport.

Ms KING—In your presentation you listed the main threats to aviation security. It may be a little difficult for you to answer this, but what do you think are the main threats to aviation security here in Australia?

Mr Meital—I do not have any idea about the intelligence picture here in Australia. That belongs to the intelligence organisation in Australia. It has to give the threat assessment. In Israel the intelligence organisation gives the threat assessment to those who deal with aviation security. What they do with this threat assessment is to make an evaluation of the situation and, from that stage, they decide what has to be implemented and what they have to do—increase security, sometimes decrease security, put in place one more security officer here or put in place sky

marshals or other security guards all over the world and all over the sea. One thing I do not know is what the Australian government does for security of airlines that come to Australia from overseas. Who is responsible for security? Is it the local authorities? Take a Qantas flight from Paris to Melbourne. Who is responsible for security in Paris?

Senator WATSON—I think there is a weakness in using the analogy of flying from Paris to Melbourne and then getting on another plane and flying from Melbourne to the United States without going through security again.

Mr Meital—I do not understand your question.

Senator WATSON—If a person flies from an overseas destination, say, into Melbourne or Sydney and does not leave the terminal and immediately boards another flight, say, to the United States—

Mr Maor—Is it a threat?

Mr Meital—Yes, it is a threat—and who is responsible for this threat?

Ms KING—In your experience, who generally pays for the technology and the manpower to improve aviation security in the areas you have been involved in?

Mr Meital—In Israel the government funds aviation security by 50 per cent, and all the rest falls to the airlines and the airport authority.

Ms KING—Could you be a little more specific about that? What does 50 per cent mean in terms of the government's contribution? What core things does it do?

Mr Meital—For the airline budget it is something like $60 million a year.

Ms KING—What sorts of things are the responsibility of government—

Mr Meital—Manpower, technology and the seats of the sky marshals.

Ms GRIERSON—Were you present this morning during the presentation by the union and the owners of Melbourne airport?

Mr Meital—We entered in the middle of the presentation.

Ms GRIERSON—Would you like to give us an assessment of what you would see as the state of security, given that that incident involved the breaching of several alarms and a 30-minute delay before anyone responded? What recommendations would you make regarding that?

Mr Meital—There is the question of building and formulating a security system. You would have to have drills and exercises to train people; they have to learn in the field. It is something that has to be trained for.

Ms GRIERSON—You asked us who is responsible when people fly from Australia to, say, Israel.

Mr Meital—No, from Paris to Australia.

Ms GRIERSON—From Paris to here—whatever. Melbourne airport suggested they coordinate security but are not responsible for everything. How do you overcome the fact that an airline operator sees their role in one area, that the whole airport manager sees it separately and that lots of it is devolved? How do you get a holistic approach?

Mr Meital—I think it can be done in Australia. In Australia you need one organisation, one apparatus, that will deal with aviation security. But overseas every airline has to be responsible for security for its own flights according to the direction of one organisation here in Australia.

Ms GRIERSON—But when it lands at Paris airport it depends on somebody else. Is that right?

Mr Meital—No. It can depend on the local authorities, the French people, but they must have guidelines and their security personnel to deal with that specific flight.

Ms GRIERSON—Are you involved in training of security personnel?

Mr Meital—We can do training of security personnel. That is what we did in Israel. In Israel, everything is centralised. One organisation does the recruitment and the training.

Ms GRIERSON—Have recruitment practices changed very much? Is there a high requirement now for security checks and skill?

Mr Meital—All the time.

Ms KING—Who owns your airports?

Mr Meital—The government; they are not privatised.

ACTING CHAIR—How many airports are there?

Mr Meital—We have one big airport and also domestic airports in Tel Aviv, Haif, Eilat and near Aqaba, but nothing to compare with Australia.

ACTING CHAIR—No, we have 240-something.

Ms GRIERSON—Are you taking precautions regarding MANPADs—handheld missiles—in Israel?

Mr Meital—Yes. We are taking them into consideration. We do not have an answer yet, but the government of Israel has spent a lot of money to enhance the research to give us the answer to this problem. There is a technological answer that might be certificated in six months.

ACTING CHAIR—Do you mean something that can be attached to an aeroplane—an anti-missile device?

Mr Meital—Yes.

Ms GRIERSON—Have you introduced a smart card type passenger information system?

Mr Meital—Not yet. We know the ICTS technology, and it is very smart.

ACTING CHAIR—Is there any consideration of introducing that in any airports?

Mr Meital—In the future.

Ms GRIERSON—Do you think that commercial security systems like those you have put in place are affordable in places like Australia where market size and travel numbers are much smaller? Are they commercially viable?

Mr Meital—Security is very expensive. We do not have a choice other than to spend money on it, unfortunately.

Mr Maor—One of the issues that has been raised in recent times in the world is how much an individual is willing to pay for the so-called comfort level of security. It is such an elastic curve. People will pay for the comfort level if it is safe and secure. What is the alternative? The alternative is a non-secure flight or airport. If there are a few holes or gaps, customers will start to avoid that company or that airport. It is happening in quite a few airports around the world.

Mr Meital—Security is a service that you have to give to the passenger.

Ms GRIERSON—You must have done risk analysis since September 11.

Mr Meital—Yes.

Ms GRIERSON—You must have looked a lot of incidents. Are they linked to identification of passengers or to hardware and things brought on planes?

Mr Meital—Passengers and items.

Ms GRIERSON—So you cannot break it down in any way?

Mr Meital—I see many security officers making a lot of effort concerning passenger screening, but nobody checks the catering. A bomb could come from the catering, not only from the passengers.

Senator WATSON—In your submission, you point out that under the current arrangement DOTARS is responsible for aviation security while CASA is responsible for aviation safety. You state that this situation is responsible for the delayed deployment of secure flight deck doors on

passenger aircraft. Would you brief the committee on the nature of the delay and its consequences?

ACTING CHAIR—That is not their submission.

Mr Maor—I do not think that is our submission.

ACTING CHAIR—Do you have a view about the security doors into the cockpit?

Mr Meital—Yes. Maybe this is the connection between security and safety, because if you want to put an armoured door in the plane it is not a simple issue. The door has to be certified by the safety air organisation. So this is maybe the connection between safety and security. We in Israel, before September 11, found it very necessary to put in these armoured doors, and there are Israeli companies that are expert in these things, but it took us a long time to get certification from the safety aviation organisation.

ACTING CHAIR—How much do they cost?

Mr Meital—I do not know. I cannot give you the exact price, but I can check it and give you that.

ACTING CHAIR—No, that is okay; I am just comparing. You mentioned that there should be greater deployment of overt security as a deterrent, such as uniformed security personnel, passenger and vehicle screening, patrols, checkpoints and surveillance equipment. How much of that do you see in Australian airports at the moment and how do you think Australian passengers might react to that sort of increase in security?

Mr Meital—I think that the passengers will appreciate it. The combination of security people in uniform and security people under cover is very important. To deal with suspicious people or phenomena, sometimes you have to be under cover all over the area. It is a whole security plan: you have to put people all over the airport to foil any possibility of an attack.

ACTING CHAIR—You recommend the deployment of skilled security officers aboard flights. What percentage of flights do you think should have security officers on board?

Mr Meital—We use security officers on every flight. There is no Israeli commercial flight that does not have security officers.

ACTING CHAIR—What sort of weapons do they have?

Mr Meital—They have a nine millimetre calibre Glock—an Australian gun.

ACTING CHAIR—Do you not worry about aircraft decompression, if they shoot through a wall or something?

Mr Meital—No, it has been checked. Anyway, the sky marshals are very well trained. They have a special training program which is very, very difficult.

ACTING CHAIR—Have you ever had an incident in Israel where a sky marshal has shot someone on board a plane?

Mr Meital—In years before, but not with this gun; it was a much smaller calibre. It was the year before. The last attempt to hijack an Israeli plane—which was en route from Tel Aviv to Turkey—was I think 10 months ago, but the sky marshal controlled the hijacker by force without using a gun.

ACTING CHAIR—You say that enough testing has been done that you are confident, if a bullet should go astray, that you would not suffer decompression in the aeroplane?

Mr Meital—Yes, we checked it, and it has been certified by the safety organisation in Israel.

ACTING CHAIR—You mentioned earlier the aircraft protection anti-missile defence system. Have you any idea what that is going to cost? That is one of the things that has been raised constantly in Australia.

Mr Meital—About $1 million for the whole device.

ACTING CHAIR—That is a lot less than the estimate of $6 million or $7 million that we were hearing. Who will be manufacturing that system?

Mr Meital—The Israeli Elta company, which is a subsidiary of the Israeli aviation industry.

ACTING CHAIR—Does that work with new generation missiles as well as older ones?

Mr Meital—No, only those that follow the heat of the engines.

ACTING CHAIR—The old ones?

Mr Meital—Yes.

Ms GRIERSON—I apologise if you answered this while I was out of the room, but you said that Australia could be more vulnerable than the UK and the US. Did you want to say why that may be so?

Mr Maor—We do not know; we were just looking at page 3 of yesterday's *Australian*. There is no doubt in our minds that it is better to look at the very comprehensive, holistic solution to any threat. It does not matter whether we are—

Ms GRIERSON—So you provide diplomatic advice as well, do you?

Mr Meital—That is the situation all over the world now. Maybe it is a war between civilisations or something like that.

Mr Maor—Unfortunately, that is the situation.

ACTING CHAIR—Thank you both for appearing before the committee today. If we have any further questions for you, I ask whether we can put those questions in writing.

Mr Maor—Yes.

ACTING CHAIR—Is it the wish of the committee that the document entitled *PowerPoint presentation on aviation security* presented by ToLife Technologies be taken as evidence and included in the committee's records as exhibit No. 6? There being no objection, it is so ordered.

Resolved (on motion by **Senator Watson**):

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 3.47 p.m.