



COMMONWEALTH OF AUSTRALIA

# Official Committee Hansard

PARLIAMENTARY JOINT COMMITTEE ON LAW  
ENFORCEMENT

**Reference: Adequacy of aviation and maritime security measures to combat serious  
and organised crime**

FRIDAY, 18 FEBRUARY 2011

CANBERRA

BY AUTHORITY OF THE PARLIAMENT



## INTERNET

Hansard transcripts of public hearings are made available on the internet when authorised by the committee.

The internet address is:

**<http://www.aph.gov.au/hansard>**

To search the parliamentary database, go to:

**<http://parlinfo.aph.gov.au>**

**PARLIAMENTARY JOINT  
COMMITTEE ON LAW ENFORCEMENT**

**Friday, 18 February 2011**

**Members:** Senator Hutchins (*Chair*), Senator Mason (*Deputy Chair*) and Senators Fielding, Parry and Polley and Ms Grierson, Mr Hayes, Mr Keenan, Mr Matheson and Ms Vamvakinou

**Members in attendance:** Senators Hutchins and Mason and Mr Hayes

**Terms of reference for the inquiry:**

To inquire into and report on:

The effectiveness of current administrative and law enforcement arrangements to protect Australia's borders from serious and organised criminal activity. In particular the committee will examine:

- (a) the methods used by serious and organised criminal groups to infiltrate Australia's airports and ports, and the extent of infiltration;
- (b) the range of criminal activity currently occurring at Australia's airports and ports, including but not limited to:
  - the importation of illicit drugs, firearms, and
  - prohibited items
  - tariff avoidance
  - people trafficking and people smuggling
  - money laundering
  - air cargo and maritime cargo theft
- (c) the effectiveness of the Aviation Security Identification Card (ASIC) and Maritime Security Identification Card (MSIC) schemes; including the process of issuing ASICs and MSICs, the monitoring of cards issued and the storage of, and sharing of, ASIC and MSIC information between appropriate law enforcement agencies;
- (d) the current administrative and law enforcement arrangements and information and intelligence sharing measures to manage the risk of serious and organised criminal activity at Australia's airports and ports; and
- (e) the findings of the Australian Crime Commission's special intelligence operations into *Crime in the Transport Sector* and *Illegal Maritime Importation and Movement Methodologies*.

**WITNESSES**

<b>ANASTASI, Mr Adam, Acting Chief Legal Officer, Civil Aviation Safety Authority .....</b>	<b>16</b>
<b>BRAMAH, Mr Luke, Manager, Security Assurance and Advisory, Qantas Airways Ltd.....</b>	<b>25</b>
<b>CROMARTY, Mr Peter, Executive Manager, Airspace and Aerodrome Regulation Division, Civil Aviation Safety Authority .....</b>	<b>16</b>
<b>CROSTHWAITE, Mr Roger Bertram Guy, Manager, Permission Application Centre, Civil Aviation Safety Authority.....</b>	<b>16</b>
<b>DAWSON, Mr Paul, Manager, Government and International Relations, Airservices Australia.....</b>	<b>21</b>
<b>DREEZER, Mr Steve, General Manager, Maritime, Identity and Surface Security Branch, Office of Transport Security, Department of Infrastructure and Transport .....</b>	<b>36</b>
<b>FEREDAY, Mr Peter Reginald, Executive Manager, Industry Permissions, Civil Aviation Safety Authority.....</b>	<b>16</b>
<b>JACKSON, Mr Stephen, Head of Security and Facilitation, Qantas Airways Ltd.....</b>	<b>25</b>
<b>JOHNSON, Mr Jeremy, Business Manager, Biometrics, CrimTrac.....</b>	<b>47</b>
<b>KENNETT, Ms Roberta, National Manager, Background Checking Services, CrimTrac.....</b>	<b>47</b>
<b>LANGTON, Mr Kim, Managing Partner, Australia Pacific Region, Chameleon Associates (Australia) Pty Ltd.....</b>	<b>55</b>
<b>MILLER, Mr Michael, Manager, Security and Resilience, Airservices Australia .....</b>	<b>21</b>
<b>RETTTER, Mr Paul Bernard, Executive Director, Office of Transport Security, Department of Infrastructure and Transport .....</b>	<b>36</b>
<b>ROBERTSON, Mr Peter, General Manager, Aviation Security Branch, Office of Transport Security, Department of Infrastructure and Transport .....</b>	<b>36</b>
<b>ROWE, Mr Michael, Acting General Manager, Transport Security Operations, Office of Transport Security, Department of Infrastructure and Transport.....</b>	<b>36</b>
<b>SMITH, Mr Douglas, Chief Executive Officer, CrimTrac.....</b>	<b>47</b>
<b>SUMMERS, Mr Dean, International Transport Workers Federation Coordinator, Maritime Union of Australia .....</b>	<b>1</b>
<b>van GESSEL, Ms Theresa, Manager, Policy and Legal, CrimTrac.....</b>	<b>47</b>
<b>WILSON, Mr Andrew, Deputy Secretary, Department of Infrastructure and Transport .....</b>	<b>36</b>



**Committee met at 8.52 am****SUMMERS, Mr Dean, International Transport Workers Federation Coordinator, Maritime Union of Australia**

**CHAIR**—Welcome to the hearing. I advise witnesses that although the committee prefers all evidence to be given in public requests to give all or part of your evidence in camera will be considered. Evidence in camera may, however, subsequently be made public by order of the Senate or this committee. I remind witnesses that all evidence given is protected by parliamentary privilege. It is unlawful for anyone to threaten or disadvantage a witness on account of evidence given to a committee. Such action may be treated by the Senate as a contempt. It is also a contempt to give false or misleading evidence to the committee. If a witness objects to answering a question the witness should state the ground upon which the objection is to be taken and the committee will determine whether it will insist on an answer, having regard to the ground that is claimed. If the committee determines to insist on an answer, a witness may request that the answer be given in camera.

The Senate has resolved that an officer of a department of the Commonwealth or a state shall not be asked to give opinions on matters of policy and shall be given a reasonable opportunity to refer questions asked of the officer to superior officers or to a minister. This resolution prohibits only questions asking for opinions on matters of policy and does not preclude questions asking for explanations of policies or factual questions about when and how policies were adopted.

I invite you to make a short opening statement.

**Mr Summers**—Our submission is on behalf of most of the transport workers covered by transport unions in Australia. In our submission I refer to the Maritime Union of Australia, the Australian Workers' Union and the RTBU, which is the Rail Tram and Bus Union. The Marine Power and Engineers also included their comments at the time of writing this submission, along with the Australian Transport Union Federation, which is a federation of three unions: the Maritime Union of Australia, the RTBU and the TWU. Also, the International Transport Workers' Federation.

Our submission is in three parts. We want to stress the fact that the unions throughout the whole process of the development of the Maritime Transport and Offshore Facilities Security Act, MTOFSA, and regulations, and any debate or discussion about security on the wharves or in areas of maritime endeavour in Australia—and that is in the offshore oil and gas, the ports and the ferries. They are partners in maritime security, primarily because internationally we know, through out International Transport Workers' Federation experience, that every time in every incidence of a terrorist attack transport workers are killed and hurt. So we have a vested interest and a responsibility to make sure that we are involved in the development of those instruments that protect or workers from these heinous crimes.

The second part is that we are concerned that the focus of the entire debate is now shifting away from counterterrorism—and that is the whole reason we signed up to be partners in this—to what now appears to be countercrime. Also, there are gaps in security and we have been advertising these and signing them from the rooftops. We have identified some of the most

obvious ones in the back of our submission and I would be very happy to go into those later on in our submission.

The Maritime Union is the union that has consistently gone to every single meeting set up by three governments now to deal with the development of the Maritime Transport Security Act, which has flowed on to the MTOFSA, and all required legislation and regulations. Inside of that is probably the most difficult issue for us as a trade union to counter—that is that of the introduction of background security checks under the Maritime Security Identification Card, MSIC. We have no views and we have no opinions and we have not been involved in any part for the Aviation Security Identity Card, ASIC—and, of course, aviation and maritime are very different issues and very different industries. So we are solely focused on the Maritime Security Identification Card.

We debated with industry many times for robust formats: how deep those background checks should go into workers' backgrounds given the nature of our work, the responsibilities, particularly in the offshore oil and gas and on the waterfront. It protects our borders. We know that we arrived at a position where we were confident—and at the time the government was confident—that checked workers' backgrounds to such a degree that they were no threat to maritime security in any of those areas of work. I just want to stress at this stage that the Maritime Union in particular, and different from all the other unions, considers that the MSIC has become a right-to-work card in that if we cannot have an MSIC, our members—about 12,000—unlike truck drivers, rail workers and some port workers, we cannot go to another area of work. That takes away our ability to earn money to have a job. So we have labelled it a right-to-work card. That raises a whole series of questions and responsibilities for the union to focus on every part of the development and the changes or enhancements, or whatever else happens, with the MSIC. We enlisted the assistance of Dr Mark Nolan—and we included his findings in the back of our submission—to deal with the very difficult issue of the nexus between criminality and maritime security on the counterterrorism platform.

The Office of Transport Security—when initiating amendments and what they have labelled 'enhancements' to the background security check that really came down to expanding the list of maritime security related offences—relied heavily on a report that they commissioned from GHD. That has been widely publicised but condemned by industry and condemned by the unions and condemned by—well, I am not going to put words into Dr Mark Nolan's mouth, but he makes it very clear in his submission that we think the GHD report is irrelevant. We think it is not appropriate. We think there is better information, research and reference material available, particularly with a more concurrent Australian reference.

Then we move to the gaps in maritime security, which are of great concern to us. As I said at the beginning, we are partners in security. I took the liberty of bringing a small section of our youth committee—who demanded from the youth conference some months ago to be part of this process, to understand what actually happens in the parliamentary process—to come and talk to as many members of your committee as were available last Wednesday and Thursday, and they acquitted themselves very well. They were articulate and knew better than me where the gaps in security are and how security impacts on them. They are concerned about working in a secure environment and it is in their interest. They have longer to run in the industry than I have and they will be looking after their families and their sons and daughters when I am long gone—probably when we are all long gone. They came to Canberra and gave their submissions. It was



consistent with what is here. We met with the majority of your committee and we thank the committee members that made themselves available. We got a lot out of that. Certainly, our youth committee got a lot out of it and we hope that you got something out of it as well.

I want to briefly identify some of the areas of concern to us. Everybody in maritime security who needs to have unescorted access inside a maritime security regulated zone must undergo these background checks. Some are responsible for the placing of ships and cargoes and for the coordination of which ships go to which berths, which trains go to which berths and which trucks go to which departments and depots. They are all things where effective control of cargoes and manpower on the waterfront and on the offshore oil and gas rigs are completely unchecked. We think that is a pretty obvious gap in security. If it is good enough to background-check and scrutinise those workers at the coalface then surely we have to look back a few steps and have the same level of scrutiny for those people who have effective control of all those issues I just mentioned.

**CHAIR**—They are the ones, Mr Summers, that are responsible for rostering and for a number of other areas that, for instance, a fellow operating a crane would not have any control over whatsoever.

**Mr Summers**—Indeed—employment, interviews, all of those things. I am told, with our young people coming down today, that they have the capacity to fast-track cargoes in and out of ports as well, so it is a huge concern. It is probably the No. 1 concern for us.

We are concerned about contracted security staff in terminals, with what has been described to us as sometimes poor and inconsistent training. It is the case that sometimes a security guard can work on a wharf and the next day be working in a shopping centre or at a swimming pool. We think there is a big concern there and one that needs a lot more consideration.

We are worried that Australian seafarers must undergo these background checks while foreign seafarers—working on the same trade sometimes, on coastal shipping permits—need a very cursory background check. These are people from countries that are very difficult to background-check, such as Pakistan and the Philippines. Those people can come and work on our coast, on ships that have replaced Australian ships, on what and the international industry have labelled ‘flag-of-convenience vessels’, which effectively are deregulated. These vessels are also responsible for carrying cargoes like explosive-grade ammonium nitrate around the Australian coast. While the production, storage and transport are highly scrutinised and background-checked, controlled and regulated, as soon as it comes to an Australian wharf and is handed over to an FOC ship it is completely deregulated and usually, on every occasion that we know of, to the lowest bidder using the cheapest crews and, on many occasions, substandard ships. That is borne out by AMSA detentions.

The unavailability of Australian regulated ships and cruisers is a security concern and we are very happy to see that this is the subject of the Australian shipping review. There seems to be quite a bit of movement there. With the low level of container inspections, particularly in the trans-shipment of what should be empty containers, there is no scrutiny. If a container seems light enough and is labelled as an empty container, it will come in and out, trans-shipped through different ports in the world, including Australian ports, with absolutely no visual checks.

Finally, the Trojan horse conditions: the stuffing and unstuffing of containers done in depots often outside maritime security regulated zones. These people are casualised workers with no background checking at all, deregulated and what we would label as ‘uncontrolled’. From those depots, the customs seals are applied onto the containers themselves. You do not have to have any background check to apply a seal. You just buy one and put it on a container. Then the container is completely locked and secured all the way through maritime security regulated zones onto ships and to a foreign birth and possibly to a depot that is outside another country’s maritime security regulated zone. That is a big concern.

Finally, we are concerned about comments made in the GHD report about criminal intelligence. We point to celebrated cases like the Haneef case where it seems that criminal intelligence was applied to the detriment of that entire case and a very regrettable incident it was.

**CHAIR**—It was terrorism related.

**Mr Summers**—Terrorism related, yes.

**CHAIR**—Not criminal related—terrorism is a crime.

**Mr Summers**—Exactly. I point I should have made earlier is that our mantra is that every terrorist is a criminal but not every criminal is a terrorist. There lies the area for a lot of debate, an area in great need of scrutiny.

**Mr HAYES**—You probably appreciate that the Haneef case is the genesis of this revamped committee. As a consequence of the Haneef case, having the Australian Federal Police brought under the parliamentary oversight of the Law Enforcement Committee to, hopefully, examine things like that in future, as opposed to relying on a royal commission to do it. One of the consistent things through our hearings so far is the view that the waterfront is probably the highest level of risk to the country for the importation of illicit goods. Would you agree with that?

**Mr Summers**—Given that our imports are 98 per cent over the wharf, it is hard to refute that.

**Mr HAYES**—We have been briefed on the relevance of revamped security in Sydney and following that in Melbourne. Like you, we also get to identify various gaps in security arrangements around the place. Can you give me your observations on the different levels of security that operate through Australian ports. Leaving aside Sydney and Melbourne—their security is well known—do you see large gaps in security arrangements applying elsewhere in designated ports?

**CHAIR**—Mr Summers, we have seen exposed so many times with flag of convenience ships sailors who cannot afford to go onshore because they do not earn enough money to buy a hot dog or a hamburger—an incentive for them to smuggle in illicit goods is great.

**Mr Summers**—I think you have just hit a nail right on the head about the flag of convenience crews. But if the first question was about whether the gates, locks and guard security consistent right around the coast in every single port in Australia my answer is that I do not think it is. I think there is consideration given to large container terminals—to support your case that that is

where the majority of illicit goods including drugs may come through. These are only my observations. We have no evidence and we have done no work in that area.

Yesterday I made some remarks to the Maritime Security Forum that I was aware that last week there was a cattle vessel in Fremantle with 80 crew on board, which is a very big crew. Most of them were Pakistanis and they were employed by a dodgy crewing agent in Pakistan who was paying them \$300 a month. The ITF was successful in getting the company to sign an agreement for \$1,000 a month for each of these seafarers, which is still very low by the international standard. But we found subsequently that the crew had to pay three months wages just in order to secure a job. So they had to sign their first three months wages away, and they were being underpaid by \$600 a month. So they were back to their \$300-odd a month.

These people are very vulnerable. These people are coming to and from Australian ports, being paid, being intimidated, being bullied and being forced to sign things that they would not otherwise sign. Subsequently, we are told, at least three people jumped ship. They walked up the road and did not come back. I do not think the problem is whether the seafarers will go up the road and come back; it is that they are intimidated, treated very badly and abused. We see that very regularly.

**Mr HAYES**—That must be a security risk in itself. If people are treated that badly they must be ideal targets for corruption.

**Mr Summers**—That is our point. We have made the point quite often that the flag of convenience system provides a deregulated system. Inside that system we have very bad operators working in very tough areas. Seafarers are the ones that cop it on every occasion. By ‘copping it’ I mean that I have seen crews starved and crews deprived of fresh water. Last week I saw the crew of a car vessel, who had not been paid for four months. That vessel was trading around Australia delivering luxury cars. If these people are not ripe for the picking by evildoers, then I do not know who is.

**CHAIR**—So that car vessel would come into, say, Fremantle, and then go around the coast and the union is trying to ensure that at least domestic trade is carried out by people who work under our wages and conditions. Is that correct?

**Mr Summers**—There are essentially two industries. There is an international shipping industry and a coastal industry. The government is now moving to support the coastal industry with secured, background checked, regulated Australian ships and crews and companies. However, there is an international market that is free to the rigours of the flag of convenience. In this case it was a car carrier that delivered cars to different ports. So it was not actually involved in the carriage of coastal cargos but it did visit a number of Australian ports and delivered cars as it went through. In this case, when we saw it, it was in Townsville.

**Mr HAYES**—From the union’s perspective, what level of risk do you see associated with vessels flying flags of convenience?

**Mr Summers**—I think vessels flying a flag of convenience need to be closely scrutinised. They need to be assessed based on a number of criteria. For example, a very old vessel, which has a bad detention record or has a bad record of having crewing agents from dodgy areas,

should come under closer scrutiny. I know that the Australian Maritime Safety Authority have a list and a method of choosing which ships are of greatest risk for safety issues. Perhaps the same method should be applied to maritime security. There are very good operators using flag of convenience vessels—I want to add that—which have a dignified agreement brokered with the ITF to protect the wages and conditions of the seafarers on board. Those seafarers rarely jump ship. Those seafarers are in there for a career. They want to make money and they want to be safe. They want to send money home to their families on a monthly basis. If they can do that in a safe, organised way that is protected by their union or by the International Transport Workers Federation, then that is a secure part of the industry. On the other hand, in the worst-case scenario we have seen—as I have described—people were abused and intimidated. I think there is a risk there.

**Mr HAYES**—Do you see that there is a role for further policy development in that space?

**Mr Summers**—I certainly do. I think there is an area of investigation as to where these seafarers have come from, where the crewing agents have come from and who owns these crewing agents. I do not want to identify any particular country, but we know that there are crewing agents engaged in a lot of skulduggery. If someone is involved in an industrial dispute with the protection of these seafarers, we know that their families are visited in the middle of the night by thugs. This is well documented by the ITF. These are isolated cases, but they do happen, so I think we have to focus on those vessels trading on the Australian coast and even deeper, particularly those vessels that are carrying high-consequence dangerous goods.

**Mr HAYES**—Should foreign flagged vessels, particularly those that are running cheap crews and have dodgy practices, be an area of investigation for the Australian Federal Police as well as the Australian Crime Commission perhaps, if we are going to address the issue of illegal importation of substances?

**Mr Summers**—I have not considered that question before, but certainly things that happen on board some of those deregulated vessels, in the worst-case scenario, are criminal. If they are coming to Australian shores and ports they should be the subject of Australian criminal investigations. I have witnessed seafarers being beaten and had a terrible time trying to get police assistance because they are unsure of their jurisdiction of a foreign flagged ship. On a Panamanian or Mongolian flagged vessel, who has jurisdiction? It would bear closer investigation and we would be happy to participate.

**Mr HAYES**—We have heard from law enforcement at various levels about who has jurisdiction at the ports and whether it comes under Commonwealth or state or territory jurisdiction. I suppose that is further complicated by who has jurisdiction on the vessel itself.

**Mr Summers**—I think it does, because we know from industrial and safety points of view that, once you get past the gangway, it is all very jurisdictional. As soon as you step foot on the gangway it is a different jurisdiction. We have flag state versus port state jurisdiction.

**Mr HAYES**—Maybe that is something we should be looking at. In your opening statement you mentioned gaps in security. Would you elaborate on that.

**Mr Summers**—Sure. We have listed the gaps in security at the back of our submission. I talked about the lack of background checks on some of those who are responsible for effective control of management, placement of vessels, recruitment and workers on the waterfront. So we are talking about—

**Mr HAYES**—People who can set a roster or even predetermine the location of a container, for instance?

**Mr Summers**—On a wharf there is a system of management inside the offices for where containers go, so it is not just left to a wharfie to determine where he is going to stack it at the time or have an empty base. They work out where the containers are going and where they are going to be dispatched. If they are going to be transshipped, they work it on that sort kind of basis. But my point is that those people who may work in an office outside of the security regulator's zone have ultimate control of this and ultimate control of recruitment, placement and the inner workings of a wharf, a ship or an offshore facility.

**Mr HAYES**—We have been advised that consideration of the waterfront is not just about looking at the immediate surrounds or the infrastructure of the port itself. It is also about bond stores or various forms of receivers anywhere in the country, including freight still being bonded when it is on rail, for instance, and getting opened. If you are looking at the waterfront it extends a fair way, but your members are only contained in the physical parameters of the dock area itself, aren't they?

**Mr Summers**—Yes, they are, and generally you have got a maritime security regulated zone that is identified probably by a fence, usually by a properly mapped-out zone. That is a balance, as I understand it, between practicalities and costs and operational requirements. In the case of some of our major terminals, there is a big fence that goes around the perimeter of those zones so they are clearly identified. One of the gaps in security that we have highlighted is that the packing and unpacking of these containers is done off-site, outside of those zones, by people with no background checks.

**Mr HAYES**—The other area that the committee has been alerted to relates to transport operators, drivers, coming through, some with an MSIC and others without, but if they give some explanation at the gate they are admitted, as opposed to being denied access. Is that an area that your union would see as needing tightening up? Doesn't there need to be greater vigilance about people external to the port coming through and picking up containers, in terms of drivers and their purpose for being at the port itself?

**Mr Summers**—Our members certainly have a consistent view that, if, by virtue of coming into a maritime security regulated zone, they have to meet the background check requirements and all other requirements, then everybody should. I am not aware that you can explain your way out of it and I have not heard of that happening. I have heard that people will lend themselves and their cards to sit in the cabin and go through a terminal, so that somebody else inside of the cab has an MSIC. That in itself is a bit of a problem, if somebody is sitting out the front with a shingle over their heads saying 'MSIC for hire on an hourly basis' and there is no relationship between the driver and the card.

**CHAIR**—There have been a number of instances where people say they have left their card at home in, say, Bathurst or Orange, and someone will lend them a card. Clearly, a bit more scrutiny is required if that is the case, maybe by using biometrics, as some people are suggesting, fingerprints or something like that.

**Mr Summers**—Biometrics is an area in which there has been a lot of debate internationally, and there is an international convention that deals with that—I think it is ILO Convention 184 or 185 relating to biometrics for seafarers—and that has gone through a lot of scrutiny. We are not opposed to that because you give seafarers the right, therefore, to identify themselves without carrying a passport. International seafarers have their passports put in the captain's safe, where it stays for a year, and they get it when they finish up, so it is very difficult for them to identify themselves coming through. So biometrics would help them, but there have been some problems, technical problems, with exactly how they do that in the wharf environment. But we are not immediately opposed to that idea.

**Mr HAYES**—So you would not be opposed to MSICs and ASICs, for instance, being based on biometrics to ensure that the identity of the cardholder was the person concerned?

**Mr Summers**—It is a difficult area. Again, we have to have a look at exactly what that means. In the early days of the development of the MSIC, the Australian government of the day invited some US specialists over to talk about smart cards versus what they call dumb cards and, in an amazing admission, they said that we can plant these smart cards outside a union hall and with the responders we can monitor who comes and goes. We might find out someone has a late library book, because the capacity of a smart card is such that it can access a whole lot of other databases and information centres and used for issues that are not related to maritime security. So, if it became a smart card, we would have some concerns and we would have to have a debate about exactly what that means, how far that goes. But, if it were simply a matter of biometrics, without the added dangers and concerns about smart cards, we would have a look at that for sure.

**Mr HAYES**—Okay. Thank you.

**Senator MASON**—Mr Summers, you mentioned in your submission that you are wary of or, indeed—perhaps I should put it in stronger terms—opposed to the use of criminal intelligence in determining eligibility for MSICs. You say:

... it will merely punish workers who may have offended in their past, in essence initiating double jeopardy.

Can you elaborate on that. Why do you think criminal intelligence background checks would be inappropriate?

**Mr Summers**—I think there are two questions there, Senator, with respect. The first is the double jeopardy question. People who have offended and who have paid for their crime and done their time and, hopefully, been rehabilitated through the Australian system, should be allowed, therefore, to go back into a workforce. The second is criminal intelligence, which is a completely different animal, we think. We had a look at the GHD report, and as poorly researched and as dangerous as that is, they even admitted that that was notoriously unreliable. I am quoting from memory.

The second is criminal intelligence, which is a completely different animal, we think. We had a look at the GHD report and, as poorly researched and dangerous as that is, they even admitted that that was ‘notoriously unreliable’—and I am quoting from memory.

**Senator MASON**—Criminal intelligence in a general sense—

**Mr Summers**—Yes.

**Senator MASON**—I think that it varies in its quality, I accept that, but I would not say that it is always unreliable.

**Mr Summers**—I am using the GHD report, which we are condemning anyway. But even from their perspective they are saying—

**CHAIR**—Mr Summers, you have heard of what the law enforcement agencies call the ‘Admiralty index’?

**Mr Summers**—No, I have not.

**CHAIR**—The level of efficacy of the intelligence goes from one to five, or one to six.

**Senator MASON**—It varies. I accept that if somebody has committed a crime and has been convicted of a crime in the past that should not be the end of their working life, and so forth—I accept that—and there is spent conviction legislation operating in every state and, indeed, federally.

**CHAIR**—There is no shortage of federal MPs for sentencing—

**Senator MASON**—Indeed. But to say that it is irrelevant is going a little bit too far, don’t you think?

**Mr Summers**—Throughout this whole process we have focused on counterterrorism. We have maintained, and we have argued very robustly, that the maritime security related offences, that list of offences against which we are tested when we apply for a card, should be appropriate to the task, and the task that we set out, that we supported and we partnered, was counterterrorism, not counter-criminalisation. So we have not got into the counter-criminal part of it at all. In fact we have argued against it because of the issues I raised earlier. We are partners in counterterrorism.

We have read the submissions and we understand that there is what we describe as a ‘suite’ of agencies responsible for looking at criminality all across Australian society including on the wharves, and we have cooperated in that. Nobody can say that you go to an area where the unions are involved and we shelter, hide or support criminals. We do not. It is against our culture. It is against what we are standing for. We just want to go to work safely, get a fair day’s work, and go home. That is what we are about and we really take offence to some of these front-page ridiculous claims. Even *Four Corners* has made ridiculous claims. The *Four Corners* program—and I forget the journalist who made these accusations—knew of criminal cells working on the Sydney waterfront. It just begged the question that if they know of it, then surely

the police know of it and they can go and arrest them. So it just beggars belief. We are very concerned about the hysterical—

**CHAIR**—Maybe the police do know of it but they do not have enough evidence to get them.

**Mr Summers**—Well, we are not standing in the way and I do not think that the MSIC is standing in the way either.

**Senator MASON**—It is just that we have heard evidence that with serious and organised crime there are connections with people who work on the wharves—not just unionists but across the penumbra of people who work on the wharves—and we need to enhance the integrity of the card. Criminal intelligence is a very important part of that. To attempt to divide, on the one hand, antiterrorism from serious and organised crime, even as a matter of theory, is difficult I think—and I had a look at Dr Nolan's paper before. Even the former Prime Minister, Mr Rudd, said that serious and organised crime can in fact fund international terrorism. In other words, I think that it is pretty hard conceptually, Chair, to pull the two apart. So I am not convinced of your objection to more significant checks and the use of criminal intelligence to decide who should have access to certain positions on the wharves. I am not yet convinced.

**Mr Summers**—Dr Mark Nolan has done a little bit of work in this area at our request. He basically addressed the GHD report for us because that was the basis on which the Office of Transport Security was making changes to the MSIC. I have not heard anyone say that the integrity of the card is low, bad or irrelevant. I think the relevance of the card and the relevance of the background checks are what are important. When we get right to the core do we separate criminality from counterterrorism? I do not think we can say, 'You can't separate it' or 'You can separate it.' We say that we are focused. We will have put all of our energy, money and resources—we have attended every single meeting—on the basis of counterterrorism and making sure that the integrity of the card is relevant.

**Senator MASON**—It is not so much the integrity but enhancing the utility, which is a slightly different issue. I think people have said you enhance the utility of the card through greater criminal intelligence. It was some the evidence. I am not saying you have to agree with it, but that is a lot of the evidence that we have heard. You have mentioned Dr Nolan's report. Let me just read a part of it. Do you agree with the following?

... a range of demographic and individual characteristics ... may affect the likelihood that an individual may be engaging in an active criminal career—and thus be considered a risk to maritime security.

**Mr Summers**—I have not got that in context, but I have had a number of discussions with Dr Nolan and he was concerned that we do start to get into the area of profiling. Correct me if I am wrong, but I think that is what you are alluding to. Profiling, based on the criteria you have just mentioned, is extremely dangerous, especially in a multicultural country such as ours.

**Senator MASON**—The problem is the 'a range of demographic and individual characteristics may affect the likelihood.' Dr Nolan is not right. I will give you an example: the most significant demographic, social or biological fact about criminality is the gender of the individual.

**Mr Summers**—I was not aware of that.



**Senator MASON**—Being male is, and then age becomes secondary and so forth. I happen to be a criminologist, so I read this report with some glee. I do not agree with it. He is entitled to his opinion. He is an academic at the ANU—a great university—but I think some contention could be taken with Dr Nolan’s report, let me just alert you to that.

**Mr Summers**—Sure. It is a shame Dr Nolan is not here. He told me he could not make it.

**Senator MASON**—I am not suggesting that I disagree with everything, but even his comment on page 11 of his report, where he says:

This work asks what role societal treatment of groups perceived to be at risk of radicalisation has on their movement towards extremist behaviour. This work takes us beyond more simple notions of predicting risk based on prior offending and individual characteristics alone. It examines the dynamic social forces at play when law reform and institutional decision-making is perceived to be fair, or not, by those already at some stage in the radicalisation process.

I think what Dr Nolan is trying to say is that individuals might not be responsible but that societal pressures may somehow influence someone’s radicalisation and, therefore, potential terrorist activity. There would be plenty of people who would say that there is a lot more than societal pressures at play. Anyway, that is a criminological debate.

**Mr Summers**—That is right—and one I am not equipped or qualified to entertain. We got the best and most appropriate person that we could find and we were very happy with his reports and work. We will go back and talk to him about how we can further our arguments, but I am not a criminologist or an academic. I am a seafarer by trade. I know what happens on the wharf, on ships and in the offshore oil and gas industry. I can assure this committee that it is not cloak and dagger, and that there are not gangsters and criminal lurking in every corner.

**Senator MASON**—I used to teach criminology and I always used to say to people that the step from teaching criminology into parliament is but a small one.

**CHAIR**—You talk about criminal intelligence and in the second paragraph you say:

... the GHD report is rejected by unions as divisive, unreliable and counter productive ...

You then say:

This kind of evidence has been responsible for targeting union officials as described in the TWU submission and is notoriously unreliable.

I should declare that I am a life member of the TWU. I am assuming on that basis that there is a concern because union officials would need, say, an ASIC or an MSIC. In the case of the TWU one Qantas was the issuing agent for the ASIC and the TWU, as I recall, wanted to highlight the fact that anybody could use the card to bring people in to Sydney airport and they brought in a photographer from the *Daily Telegraph*. I think the card was suspended or cancelled. One might say that is a legitimate union activity, one might not. I am not sure that official had his right of entry withdrawn. It maybe unfair at this stage to highlight that with you. Could you take it back to the office and ask for an opinion as to whether or not an ASIC being withdrawn is the same as effectively withdrawing the right of entry authority?

**Mr Summers**—I would say very clearly it would not. The requirement for an ASIC in this regard is similar to MSIC.

**CHAIR**—You have currently before Fair Work Australia haven't you one of your officials at Sydney port who has been challenged by Patrick's I understand to take away his right of entry?

**Mr Summers**—That is right.

**CHAIR**—But he never had his MSIC challenged that you are aware of?

**Mr Summers**—It was not challenged and the MSIC is in this instance very separate from industrial right of entry. To answer your first question, if somebody lost their MSIC, you would have to ask why they lost it in the first place, but their right of entry would not necessarily be revoked because they could still have right of entry going in with somebody else who does have an MSIC and being in constant view of and contact with that person. For example, if you do not have an MSIC now, you can go onto the wharf. I think you went for a tour in Adelaide on Monday. You did not have to have an MSIC because you were with somebody who did, so you are covered under those areas.

**CHAIR**—We arrived with a lot of Federal Police as well.

**Mr Summers**—I am not sure all those are beyond reproach because there has been some press about the Federal Police being infiltrated as well.

**CHAIR**—Almost as much as about MUA members!

**Mr Summers**—Exactly, but we do share a common area down on the waterfront quite often. Those two are different areas. Right of entry is based on industrial requirements, doing the test and doing other business, we all have a right of entry to facilitate. My ITF inspectors do as well. An MSIC is quite different and an ASIC is as well. In the case of our Sydney official that has been settled and it is not an issue.

**CHAIR**—That was in the court for about 14 days wasn't it?

**Mr Summers**—Yes, but I checked before I came in and it has been settled.

**CHAIR**—So he did not have his right of entry revoked or anything?

**Mr Summers**—No, it has been amicably settled by all players.

**CHAIR**—Okay. In your submission you highlight the gaps in security. The security staff at ports are contracted.

**Mr Summers**—As I understand it they are all contracted. I am not aware of anyone who has their own security staff.

**CHAIR**—And they are not covered by the MUA, are they?

**Mr Summers**—No, they are not. I think in one or two areas they may be. I cannot be relied upon. I am not sure.

**CHAIR**—I imagine in a number of ports when Customs decides to target particular containers your members are the ones that unstuff and then stuff them again. At Sydney I think the acronym is CEF.

**Mr Summers**—I am not aware of that. I am not sure.

**CHAIR**—In terms of gaps in security your submission relates in large measure to seafaring rather than the port side. From the union's point of view is that where you see the significant gaps in security are—on the water rather than on land?

**Mr Summers**—No, we think it is a combination. We cannot say it is just wharves, docks and ships, because there are maritime security related issues on board the offshore oil and gas industries which are floating production facilities that never move; they stay at anchor for their entire life. There are some issues there. Our major core issue, as I have said a couple of times already, is that there should be a consistent level of security background checking for those who have effective control of management and of cargoes on the wharves. That is a landside issue as well, but there is an international perspective with carriage of high-consequence dangerous goods by cursorily checked seafarers on the Australian coast participating in the Australian coastal industry.

**CHAIR**—The final point in your submission on gaps in security is the trojan horse concerns around the stuffing and unstuffing of containers by unchecked staff outside of the security regulated zones. Please expand on your concerns about that.

**Mr Summers**—Sure. In conjunction with an initiative of the Transport Workers Union, the Maritime Union of Australia and the RTBU which is the transport union federation, we have focused on the issues industrially and security-wise around container depots and those that are outside of maritime security regulated areas. These could be out in the suburbs, but as long as they are outside of the fence or the zone itself then they are under some sort of scrutiny.

We know this is a largely casualised area, so low-paid and non-organised workers come in there to open the containers, stuff them or the goods are sent to a container yard because sometimes you might not have enough goods to send in one container so the company will organise to send a whole lot of people's stuff in one container. These people stuff those containers and then are responsible to put a security seal on that container and send it into a security regulated zone.

**CHAIR**—From your years as a seafarer and now as an MUA official, is there anything we can do to protect the integrity of the seals on containers? We have had evidence given to this inquiry of people breaking the seals and no-one gives a continental and that replacement seals are available if they are needed. Is there anything that you have seen that can make sure that when that container gets to its destination it cannot be tampered with?

**Mr Summers**—No.

**CHAIR**—That is not very encouraging.

**Mr Summers**—I think it is a technical question. There may be advances in the area of some form of electronic protection for those containers. It is not my field, but we do think that if you have a look at maritime security from where a container comes inside the gate to where it leaves the other gate in whichever country that is, that is an entire corridor of maritime security. Everybody is background checked in one way or another through maritime security. It is very, very strong in Australia. In fact, the MSIC leads the world by a long shot.

**CHAIR**—Is it stronger than the US and Canada?

**Mr Summers**—Absolutely. We have travelled to these countries, spoken with government officials, unions and other workers in the area and we found that the TWIC card has enormous problems, particularly on the West Coast of the United States where a lot of the drivers are from Mexico. From Los Angeles to Long Beach there are 200,000 truck movements a day. I think the general consensus is not all of them are done by US citizens, so how do they background check those people? In Canada there are still problems with their card—I forget its acronym. But Australia stands out, probably by virtue of the fact that we are an island nation and that we do have a very high level of security and very high-tech wharves and things like that. We stand out around the world as being outstanding in the Maritime Security Identification Card.

**CHAIR**—One of the things we heard yesterday is more evidence of the street price of a number of the drugs that come into this country and the temptation from that. We have the deputy crime commissioner from New South Wales on remand at the moment for allegedly being involved in the importation of amphetamines, I think. We have army officers in jail because of corruption. We have senior figures who pledge themselves to the Queen and all the rest of it and are either on remand or in jail.

I do not know if you would be aware of the street price or the wholesale price of, say, cocaine, here in Australia. I am sure you wouldn't. Cocaine, heroin, amphetamines—it is just staggering the amount of money that any enterprising criminal who wanted to take that risk could make. I would be astounded that anywhere in the supply chain that there would not be figures from drivers to maritime workers that would not be involved. Would you have a comment on that?

**Mr Summers**—I think you have just identified that it is much broader than the supply chain. Every area of society in the world has a capacity—

**CHAIR**—I am just saying that the incentive is there. The wholesale price of cocaine in Australia I think is nearly \$200,000 a kilo and the retail price is over \$300,000 a kilo. So, if you get 40 or 400 kilos through, you can retire to Potts Point, Point Piper or wherever all those other eastern suburbs criminals come from, which are generally represented by the Liberal Party, of course!

**Mr Summers**—I have no idea of the street price of those drugs. I think your other questions are probably better targeted at a criminologist.

**CHAIR**—Fair enough. Thank you very much, Mr Summers.

**Mr Summers**—Thank you.

[9.47 am]

**ANASTASI, Mr Adam, Acting Chief Legal Officer, Civil Aviation Safety Authority**

**CROMARTY, Mr Peter, Executive Manager, Airspace and Aerodrome Regulation Division, Civil Aviation Safety Authority**

**CROSTHWAITE, Mr Roger Bertram Guy, Manager, Permission Application Centre, Civil Aviation Safety Authority**

**FEREDAY, Mr Peter Reginald, Executive Manager, Industry Permissions, Civil Aviation Safety Authority**

**CHAIR**—I welcome officers of the Civil Aviation Safety Authority. I now invite you to make an opening statement, at the conclusion of which members of the committee will ask you questions.

**Mr Fereday**—I have an opening statement which has been provided to the secretariat. Would you like me to read it out?

**CHAIR**—Yes, thank you.

**Mr Fereday**—The purpose of this opening statement is to inform the committee of CASA's role generally and in relation to aviation security. CASA is a Commonwealth statutory authority established by the Civil Aviation Act 1988. CASA's main function is to conduct the safety regulation of civil air operations in Australian territory. In exercising its functions under section 9A(1) of the Civil Aviation Act, CASA is required to regard the safety of air navigation as the most important consideration.

In relation to aviation security, when the Civil Aviation Act was enacted, section 9(5) of the act stated:

CASA's functions do not include responsibility for aviation security.

This subsection was repealed by the Aviation Security Amendment Act 2004. The explanatory memorandum to the bill for this act explained this was done:

... to remove any possibility that CASA is precluded from taking on some security functions.

On the Aviation Security Identification Card, CASA is one of approximately 50 issuing bodies for ASICs. The Aviation Transport Security Regulations 2005, the ATSRs, state that CASA 'is an issuing body' in regulation 6.12A of that ATSR.

The Civil Aviation Act empowers regulations to be made to formulate a scheme in relation to security status checking, though such regulations have not been made under the act—regulations appear in the ATSR, so we utilise those. The ATSR confer upon CASA the function of

determining, under subsection, 74G(1) of the Aviation Transport Security Act, that a person has an adverse aviation security status. That is in 6.55A of the ATSR. An aviation security status check of a person includes: if the person is not an Australian citizen, a check as to whether the person is an unlawful noncitizen; a check of police records to find out whether the person has a criminal record; and a security assessment. That is under 6.54 of the ATSR.

On requirements in relation to the issue and use of flight crew licences, the status check which I just mentioned is necessary because the ATSR state that CASA cannot issue a pilot licence to a person unless: the person has their identity verified by CASA, an aviation security status check has shown that the person does not have an adverse criminal record and CASA has been notified in writing that a security assessment of the person has been made and is not adverse or qualified. That is in 6.57 of the ATSR. A person who is over 18 and holds a pilot licence must not perform a duty that is essential to the operation of an aircraft while the aircraft is in Australian territory unless: his or her aviation security status check is current, or he or she has requested an aviation security status check. That is in 6.55 of the ATSR. This is the extent of CASA's functions in relation to aviation security.

Regulations 4.67 and 4.68 of the ATSR impose requirements on certain aircraft to have a hardened cockpit door. CASA has on occasion considered issues as to whether those doors meet aircraft certification standards.

On aerodromes, regulation 139.040 of the Civil Aviation Regulations 1988, which we call CASRs, provides a person must not operate an aerodrome that has a runway suitable for use by aircraft with a maximum seating capacity of more than 30 seats or maximum carrying capacity of more than 3,400 kilograms, which is available for use in regular public transport or charter operations, unless the aerodrome is a certified aerodrome. CASA will issue an aerodrome certificate if the aerodrome meets prescribed facility and equipment standards, the aerodrome has satisfactory operating procedures, an aerodrome manual has been prepared for the aerodrome and the applicant for the certificate would be able to properly operate and maintain the aerodrome. That is under 139.050 of the CASRs. Otherwise, in general, a person can land or take off from any place so long as it is suitable for use as an aerodrome for the purposes of the landing and taking-off of aircraft That is in 92(1)(d) of the Civil Aviation Regulations 1988.

Any such place may be, but does not need to be, registered as an aerodrome under part 139 of the CASRs part 139. When registering or certifying an aerodrome, CASA does not assess any aviation security issues, although CASA will assess an aerodrome emergency plan for a certified aerodrome—that is in 139.210. This is separate to a Transport Security Program, which some aerodromes are required to have, but the Department of Infrastructure and Transport deal with these.

CASA does not have a role in monitoring aircraft movements across the borders of Australia. However, certain aircraft operations into Australia require the permission of CASA, which is covered by sections 25 and 26 of the Civil Aviation Act. From time to time, sharing of information with law enforcement agencies is required. CASA receives requests for information about pilot licensing and aircraft registration status from Commonwealth and state law enforcement bodies. When we receive such a request, as long as it is not prohibited by the Privacy Act, CASA will provide the information sought.

Today I have with me colleagues who will be able to help in the areas of the issuing of the ASICs and with any questions about aerodromes and legal requirements.

**CHAIR**—Thank you. The committee has had an opportunity to go to Jandakot Airport, and my question is framed in relation to what has happened there in terms of criminal activity, particularly in domestic drug distribution, using small aircraft and landing strips. Does CASA have any regulatory powers relevant to the control of such activities?

**Mr Fereday**—No.

**CHAIR**—What sort of powers could be used to ground an aircraft, prevent it from leaving, with people on board who are suspected of criminal activity?

**Mr Fereday**—Our powers are restricted to the airworthiness of the aircraft, the qualifications of the flight crew and the suitability of the aerodrome. That would be a police matter.

**CHAIR**—You do not have any sanctions that could be used by law enforcement agencies to assist them where they suspect that criminal activity is about to occur, rather than there being contraband or drugs on that small aircraft?

**Mr Anastasi**—CASA has no specific powers to assist a law enforcement agency in that manner. We could not ground the aircraft to facilitate the law enforcement agencies accessing the aircraft and searching it.

**Senator MASON**—You ‘could not’?

**Mr Anastasi**—That is correct.

**Senator MASON**—Does that mean you do not have the legal power or that you choose not to?

**Mr Anastasi**—The powers that CASA has are granted upon safety so, unless there is a safety basis to take action, it would not be appropriate for CASA to exercise those powers.

**CHAIR**—In relation to international small aircraft movements do you have any additional powers or sanctions you could use other than airworthiness, crew training or whatever? In particular we are looking at Northern Australia, coming out of New Guinea or Indonesia.

**Mr Anastasi**—By way of background, in relation to what aircraft do come in, there are obviously different classes of operation. There is commercial operation of aircraft and there is also private operation of the aircraft. Under the Civil Aviation Act, if it is a commercial operation the aircraft requires permission from CASA before it can come into Australian territory.

**CHAIR**—You are 100 per cent sure that every aircraft that comes into Australian territory gets permission from CASA?



**Mr Anastasi**—I have spoken about commercial aircraft. The answer to your question is yes. In relation to private aircraft, the legislation does not require permission to be obtained from CASA before the aircraft can come into Australia or depart.

**CHAIR**—To whom do they have to apply? Going back 60-odd years, if the Japanese had decided they would use private aircraft to come in to Darwin they would not have had to apply to anybody?

**Mr Anastasi**—That is correct. There may well be Customs requirements separate to that but, in terms of the Civil Aviation Act, there is no requirement.

**CHAIR**—So it is unregulated. If you want to fly out of New Guinea or Indonesia into Northern Australia, if you have a private aircraft that can fly that far, you do not need to advise anybody? You do not need to advise CASA?

**Mr Fereday**—You do, however, need to advise the Department of Infrastructure and Transport. That is not our area.

**CHAIR**—Which division is that?

**Mr Fereday**—I believe it is the National Passenger Processing Committee. It is not our area. It is really a question for the department.

**CHAIR**—I know it is not your area. If it is a private aircraft bringing in freight rather than passengers is there any difference there?

**Mr Fereday**—No. If they are doing commercial activity, if they are making money from bringing in freight, then they have to have an approval from CASA. But if it is not, if it is private goods, they do not have to apply to CASA.

**CHAIR**—This is an inquiry into maritime and aviation security and dealing with serious organised crime. So, if they were bringing in kilos of cocaine, heroin or amphetamines, they would have to tell you, because it is commercial, but if they said it was just for private use they would have to advise the department of infrastructure's National Passenger Processing Committee?

**Mr Fereday**—In that case, they would not be advising anyone.

**CHAIR**—That does not seem all that adequate. Has CASA made comments about whether they should be dealing with this aspect of international small aircraft movement? If you have not or if it is something you want to take on notice, you can.

**Mr Fereday**—I think so. In our opening statement we said our chief concern was the safety of air navigation. If it does not fall under that, we would leave it to others to look after. It is not something we have been chasing down.

**Mr HAYES**—I want to ask about flight crew licences. I understand that police checks are made. A licence is issued under, I think, regulation 6.57 provided the finding is not adverse or

qualified. Does that mean it also takes into account intelligence issues, as opposed to a person having been convicted of an indictable offence or imprisoned?

**Mr Fereday**—Yes.

**Mr HAYES**—Does that mean if they have criminal associations?

**Mr Fereday**—We provide the information to AusCheck, which includes the three checks—criminal record, ASIO and immigration. Those things, we believe, are taken into account. It is not something we delve into ourselves. AusCheck looks after that.

**Mr HAYES**—And based on that you would issue the licences?

**Mr Fereday**—Yes, that is right.

**Senator MASON**—In your submission you quote the Civil Aviation Act. You say that initially there was not responsibility for aviation security. Then you say it was amended. You cite the explanatory memorandum, which says this was done to remove any possibility that CASA is precluded from taking on some security functions. Do you think you need further powers to enhance that capacity?

**Mr Fereday**—No.

**Senator MASON**—So you are happy with the legislative powers that you currently have?

**Mr Fereday**—Correct.

**CHAIR**—Thank you very much, gentlemen, for coming along today.

[10.05 am]

**DAWSON, Mr Paul, Manager, Government and International Relations, Airservices Australia**

**MILLER, Mr Michael, Manager, Security and Resilience, Airservices Australia**

**CHAIR**—I welcome representatives of Air Services Australia. I invite you to make a short opening statement, which will be followed by questions from the committee.

**Mr Dawson**—We do not have an opening statement. We are happy to go straight to questions.

**CHAIR**—The committee has previously heard evidence about the use of small aircraft and regional and remote air strips and the domestic distribution of illicit goods. You may have heard this evidence earlier—it was about Jandakot. What form of monitoring of such movements currently exists? What are Air Services Australia's responsibilities in this area? What controls exist in terms of international small aircraft movement?

**Mr Dawson**—Our accountabilities in terms of the aircraft coming in and out of Australian administered airspace are limited to the safe and efficient transit of aircraft.

**CHAIR**—But isn't that what CASA just said they did?

**Mr Dawson**—We are the service provider. They set the rules; we provide the service. We provide the service on the basis of the CASA standards, which are essentially international standards out of the ICAO forums.

**CHAIR**—So you would make sure that the aircraft is airworthy—

**Senator MASON**—You are talking about airworthiness—

**Mr Dawson**—We make sure that they do not bump into each other in the air.

**CHAIR**—that something does not fall off it. Is that right?

**Mr Dawson**—We keep them apart.

**Mr Hayes**—It is a good thing you do, too.

**Senator MASON**—It is a very important task, Mr Dawson.

**Mr Dawson**—It should never be underestimated, Senator. What normally happens with a flight coming in is that they will file a flight plan and we will process as they come.

**CHAIR**—They file the flight plan with you, do they?

**Mr Dawson**—Yes, they do.

**CHAIR**—If they are commercial aircraft.

**Mr Dawson**—Yes. But if they are flying in controlled airspace, they will file a flight plan.

**CHAIR**—So you do not have the same requirements CASA does, where, they said, there is a difference between private and commercial?

**Mr Dawson**—Most aircraft in general aviation file flight plans. The trouble with what the committee is looking at with small aircraft and our ability to detect or to stop is that the surveillance that civil aviation has is different to what defence has—it is a different kettle of fish. Civil aviation surveillance is primarily based on transponders on an aircraft, which send out a signal and we pick that up. That is what we call secondary surveillance technology. If an aircraft wants to come into Australia from, say, PNG or somewhere in the north, and they turn that transponder off, do not file a flight plan and land in an airport where we do not have a facility, such as a tower or something like that, I suspect we would never know about it.

**Mr Miller**—In relation, Mr Chair, to your point about Jandakot and similar airports, one thing we would say is that our staff there, the tower controllers—because we are responsible for air traffic control in such locations—do report suspicious activity, and we make those reports to the Australian Federal Police here. Clearly, it is not my position to comment on ongoing police operations, but in a couple of instances we are cooperating with the—

**CHAIR**—If you would like to go in camera—we were in camera four times yesterday—and be more explicit, you can.

**Mr Miller**—Suffice it at this stage to say that we cooperate with the Australian Federal Police and state and territory police forces where required to support the operations. There have been instances where we have reported unusual activity to the police.

**CHAIR**—Your submission notes that a number of the changes to the ASIC regime, such as expanding the relevant offence list or introducing more regular background checks, could be considered. Have there been any significant changes since the publication of your submission, and would you recommend any particular changes to the committee?

**Mr Miller**—On that point, really it is indicating our willingness to cooperate with the Australian government in ensuring that we have the most secure aviation industry that we possibly can. If I could just elaborate: we were seeking, but we did not identify that the current arrangements have any weaknesses as far as we are concerned.

To understand the personnel security of our workforce—

**Senator MASON**—Can I just interrupt—what do you mean by that? I said your submission was a wonderful submission before; your submissions are—

**CHAIR**—You said may not be sufficient, and then you went into—

**Senator MASON**—Yes, well said.

**Mr Miller**—If I elaborate on our own workforce, then perhaps you will understand it. I do not want to talk myself out of a job, but compared to my colleagues—

**CHAIR**—We can go in camera if you want to!

**Mr Miller**—in the airport and airline area, I have a much easier job in terms of personnel security. We have a workforce of about 3,600 people, and about 3,000 of those are in our key operational areas: air traffic controllers, about 800 aviation fire fighters and about 700 technicians who maintain navigation aids for the industry.

It is fair to say that we have an extremely stable workforce. You can understand this in that, if you want to be an air traffic controller or an aviation fire fighter or to maintain navigation aids, either you work as an employee of Airservices Australia or you are in the Royal Australian Air Force. There are no places to do that work otherwise. We have our own training schools for all three trades, so it is not unusual to find people who have worked for us for 30 and 40 years in our technical areas. In one case recently, a chap who is still working for us clocked up 50 years service. He started as an apprentice—

**CHAIR**—But my question to you was: since you have written the submission, have there been any changes to the ASIC regime that you would like to comment on?

**Mr Miller**—No.

**CHAIR**—You have just given us a very multi-area statement—

**Mr Miller**—I beg your pardon, I was just—

**CHAIR**—In your submission, you—not you personally, but your submission:

... notes that the current definition of ‘aviation security relevant offences’ may not be sufficient to ensure that all offences which could pose a future risk to aviation security are discovered at the screening stage ...

And then you include in that current list of offences:

... where no sentence of imprisonment was imposed (suspended sentences are however captured);

(b) offences involving firearms and other weapons; and

(c) offences contrary to the new ‘serious criminal organisation’ (i.e. anti-bikie) legislation introduced in some states.

My question to you was very straightforward, I thought—just yes or no if there has been an improvement in the scrutiny for ASIC issuances or not?

**Mr Miller**—The answer to that is—

**CHAIR**—I know you do not want to do yourself out of a job!

**Mr Miller**—That is very kind! We are satisfied with the current arrangements but would work with the Australian government if it were identified across the industry that there was a greater need. What I sought to say about our own workforce is that we are confident that we have good personnel security within our own workforce.

**Senator MASON**—Can I just bounce off that? You are satisfied with the current arrangements, and I understand that, but are you satisfied with the current legislative scheme? As the chair has pointed out, there does seem to be a gap. You may have some support in the committee for that assertion, and I suppose what the chair is asking and what the committee is interested in is if you stand by that? I think you can be—

**Mr Miller**—We stand by that statement.

**Senator MASON**—Fine. This is not having a go at your personnel at all. That is not what I am doing, nor is the chair. We just want to have a look at the legislative scheme, and if you stand by what you said in 2.1.9 and 2.1.10 in your submission that is of great interest to the committee. And you do stand by that?

**Mr Miller**—Yes we do.

**CHAIR**—Thank you very much for coming along, gentlemen.

**Proceedings suspended from 10.14 am to 10.34 am**

**BRAMAH, Mr Luke, Manager, Security Assurance and Advisory, Qantas Airways Ltd**

**JACKSON, Mr Stephen, Head of Security and Facilitation, Qantas Airways Ltd**

**CHAIR**—Welcome. I invite you to make a brief opening statement, at the conclusion of which members of the committee will ask you questions.

**Mr Jackson**—Thank you for the opportunity to appear before the committee today. The Qantas Group's main business is the transportation of passengers using two complementary airline brands—Qantas and Jetstar. The airline brands operate regional, domestic and international services through a portfolio of subsidiary businesses and employ almost 36,000 people, 93 per cent of them based in Australia.

Qantas Group airlines offer services to 184 destinations in 42 countries—59 in Australia and 125 in other countries. We carried 41 million passengers in 2009-10. Domestically QantasLink and Jetstar operate around 5,300 flights per week serving 59 city and regional destinations in all states and mainland territories. Internationally we operate more than 900 flights per week.

Safety is the Qantas Group's first priority. At the heart of our business is an unwavering commitment to world's best safety and security practices and associated reporting. As such, Qantas is internationally respected and accredited for its dedication to safe and secure flying operations. The Qantas Group does not compromise when it comes to the security of our operations, customers and employees. We work closely with government law enforcement agencies and intelligence agencies in Australia and overseas to assess and respond decisively to security issues when they arise and often to assist proactively in their prevention, to have in place robust response contingency plans and to ensure that policy and regulatory changes are implemented quickly and effectively.

As the Qantas Group business expands, our security experts continue to provide detailed analysis of new ports and business ventures to ensure that security risks are identified and satisfactorily mitigated, where necessary ensuring high standards of security are maintained at all times. Aviation security risks with the potential to impact on the Qantas Group, its passengers, its employees, its assets and indeed the community, are managed through heightened threat monitoring and assessment processes, security coordination at locations throughout the world and delivery of operational contingency plans. There is also an important security element behind exciting new customer-focused initiatives such as the next generation check-in. Professional security advice and consultation with government bodies—primarily the Office of Transport Security—and a combination of process engineering and new technology are vital in ensuring that the integrity of passenger facilitation processes is in step with innovations in technology.

Qantas recognises that serious and organised crime presents a significant challenge to both industry and law enforcement. We support the lead role played by law enforcement agencies in combating serious and organised crime and we work closely with the law enforcement community to limit its impact. Qantas has established an excellent working relationship with both domestic and international law enforcement agencies and maintains regulation interaction

with these agencies on both operational and intelligence matters. We appreciate that some employees within the aviation sector may seek to misuse their positions to perpetrate opportunist unlawful activities and facilitate criminal and/or terrorist activity. The potential for a trusted insider—airport or airline employees, contractors, subcontractors, security personnel, retailers—to circumvent security measures and to use their knowledge of the environment is an ongoing consideration for industry participants and the law enforcement community as a whole.

To assist in combating the threat posed by trusted insiders, Qantas has held a longstanding view that a strengthened Aviation Security Identification Card and ASIC regime should include a criminal intelligence check as an additional dimension to the existing range of background checks—as you know, criminal history, conviction, citizenship, national security or PMV checks are conducted by ASIO—together with a process to deliver live checking of a person’s criminal convictions against their ongoing eligibility to continue to hold an ASIC.

Qantas believes it is critical that state and federal law enforcement agencies and the aviation and maritime industries work closely together to identify and address the vulnerabilities that have the potential to contribute to criminal behaviour. There are, however, significant legislative impediments to truly achieving this objective—for example, secrecy provisions in bodies of law like the Australian Federal Police Act 1979 and the Australian Crime Commission Act 2002. These impediments, however, are not impossible to overcome, with precedent being previous albeit ad hoc partnerships between private sector companies and law enforcement agencies through the swearing in of private sector individuals as special members of those agencies.

In summary, although Qantas has established excellent working relationships with both domestic and international law enforcement agencies, we believe that these relationships would be strengthened by a greater focus on the timely, sustainable and systematic sharing of criminal intelligence and information. Qantas suggests that both public and private sector organisations and agencies could achieve this by coming together through a series of high level forums to define a road map, to make decisions and to implement practical and sustainable strategies for improved collaboration and improved private and public sector partnerships to contribute further to the fight against serious and organised crime.

That completes my opening statement, but I draw your attention to some factual pieces in the original submission that I would like to update. On page 4 of our original submission, in reference to Aviation Security Identification Cards, we said that there were some 130 issuing bodies in Australia. Today there are 183 authorised bodies, but only 67 of those bodies actually issue ASICs. On page 5 of the original submission, in the paragraph immediately under the dot points, we say that Qantas currently has 32,465 ASICs on issue, with only 21 applications having been denied. Today, as a result of proactive work that we have done internally, we have reduced the number of ASICs on issue to 24,000, and over the last 18 months 49 applications have been rejected. On average we are seeing a turnaround of four working days by government agencies, which in Qantas’ view is acceptable.

**CHAIR**—You have supplied us with a supplementary submission, which in effect relates to the public hearing the committee conducted in Perth, where a number of serious issues were raised by the Western Australian police and an academic was commissioned to look at e-tickets and the ability of serious and organised criminal figures being able to travel freely on domestic



aircraft. There has been some comment about that fact. Can you talk to your additional submission so that when we do get an opportunity to ask questions we can deal with that.

**Mr Jackson**—Thank you for the opportunity to provide the supplementary submission. The bottom line is that we felt that the next generation check-in and e-check-in environment is a relatively new innovation. It is quite complex, and obviously it is not the primary business of the law enforcement community to deliver products against the next generation check-in. We have found that some of the information was largely based on perhaps an incomplete understanding of the mitigants that we had in place to address some of the matters that the committee heard about in evidence, particularly where witnesses contended that those vulnerabilities were unacceptable for application in the aviation setting.

**CHAIR**—As you would have read in the *Hansard*, the Western Australia Police were very adamant about the loopholes in security. They did deal with criminals who had false identities or who had obtained tickets to travel domestically as a result of false identities.

**Mr Jackson**—Yes, that is correct. My view is that some of the material presented by some who are my former colleagues in law enforcement—

**CHAIR**—So you are ex-AFP?

**Mr Jackson**—I was AFP for 22 years prior to joining Qantas six years ago. Some of the factual information given to the committee was wrong. I cannot rebut the fundamental issue of identity verification in the domestic airstream. That is an issue that has been afoot for many years. I absolutely and unequivocally accept that law enforcement agencies would prefer, from an intelligence perspective, to see an outcome where we verified identity in the domestic setting.

**Mr HAYES**—Which is where the rest of the world, whether it be Europe or America, is already at with domestic flights. You demonstrate our identity a number of times just before you get on the aircraft.

**Mr Jackson**—Sometimes it is inconsistent in terms of what identity we ask for. There are neither legislative nor policy directives mandating a check-in agent.

**Mr HAYES**—Is this just a cost matter? Not all that long ago I fronted up. I had to go on the outward leg. I went up to the counter to get my ticket and showed my driver's licence. On the homeward leg I did not do any of that.

**Mr Jackson**—It is not a cost measure. The reality for us is that our staff are not trained to recognise fraudulent documents. There is an inconsistency in the ability for some of our customers who are travelling with us to produce identification. Some of them do not have photographic identity. We often carry the elderly who have never held a photographic identity card.

**Mr HAYES**—And that is why they have measures other than driver's licences. I think you can cut through whether it is cost reduction or not. Those of us who travel and travel internationally know the extent of verification that is being applied with regard to domestic and international travel. This is something that has been introduced. What the police are saying—by

the way, it was raised again yesterday in the hearings—is that it is, in terms of serious and organised crime, a matter of looking at detecting the movements of not only known criminals but also their associates in one port where drugs or other contraband may be received and not knowing where they are flying to. I think the cops over there in Western Australia made a pretty fair point on all this.

**Mr Jackson**—I accept that, but I do not accept that it is a cost measure. It is not a cost measure.

**CHAIR**—To follow on from Mr Hayes's question, one of the things that may be alluded to—I think it is in your submission—is the need for greater communication between the airlines and the law enforcement agencies. I do not know how many times it has been highlighted to us that the police want to know where such-and-such is travelling and when it filters through the system the figure that they have some interest in has already left, landed and taken off again. It seems to me—my colleagues will correct me if I am wrong—it all depends on the nature of the relationship between the law enforcement agencies at that particular airport and Qantas or whoever else. If they do not have a good relationship, they will let them know when it suits them. If they do, everything works very well. I know you are ex-AFP, so you might be able to give us a view from that perspective.

**Mr Jackson**—I will cut to the chase. I am prepared to unequivocally rebut any evidence given that there is a commercial driver behind any perception of a delay in information being provided to police. With your indulgence, I can give you a live example from last night.

**CHAIR**—I did not suggest that. In our journeys across Australia we have come across shopping malls in international airports that never would have been considered once upon a time. We know that you can get a bus from here to Sydney for \$25, but it was \$78 or something to get an airplane. Why would you compete with that sort of market? We understand. I am not being critical; we just know that these cost pressures are there.

**Mr Jackson**—Of course there are cost pressures, and obviously Qantas is not a security company that flies airplanes. My mandate is to provide value to the business, and value to the business is to assist a return to our shareholders. But with regard to any contention made by witnesses in relation to an inadequate system of real-time information, the example I was going to cite is my 24/7 security control centre. In any one year, on average we service law enforcement inquiries up to the number of 6,000. We do not charge for those. The example was given in relation to the telecommunications industry. My knowledge of interaction with Telstra in the sense of information for call charge record analysis six or seven years ago is that it was \$35 an inquiry. Last night my security controller on duty spent 70 per cent of his shift dealing with law enforcement inquiries, including a live one from the WA Police checking the manifest details of a member of an outlaw motorcycle gang travelling that evening from Perth to Adelaide. So, as Superintendent Carver can cite examples where it is not working, we can cite many examples where it is working.

Yes, you are right: often a senior constable on the ground at Perth Airport is up against a junior airport manager. The relationship is just a reality of relationships between people. But certainly at a commissioner level—certainly with Tony Negus, Commissioner of the Australian Federal Police, and John Lawler, the CEO of the Australian Crime Commission, and me—we have an

unambiguous and unconditional agreement that we ensure wherever we can the passage of real-time information to police. All we need to do is verify that you are a bona fide police officer. We do not immediately seek a search warrant, despite what Superintendent Carver contended, and I am happy to go on the public record to say that that does not signal that I am being cavalier about our legal obligations to comply with both Australian and EU privacy legislation. There are channels and parameters for us to explore making a step change in how we can improve relationships and, particularly, the passage of information to police without us going down the path of airline staff verifying identity. I am sure the committee has heard numerous times the fundamental proposition that we do not have a national identity card, so how do you verify identity?

**CHAIR**—We tried to get one once, though.

**Mr HAYES**—But your staff have been fulfilling that role for a number of years, handing tickets out across the counter on the sighting of photographic evidence that that is the person. I know that that does not necessarily guarantee against fraudulent papers, but that is something that still occurs, though on a vastly increased scale now, overseas.

**Mr Jackson**—And I agree. However—I might be guilty of splitting hairs here—that is not verifying identity. It is doing a physical—

**CHAIR**—I suppose once you get the ticket you could still give it to someone else, couldn't you?

**Mr Jackson**—Yes, you can in the domestic area.

**CHAIR**—We have been advised that if you travel domestically on a false identity there are no sanctions for doing that. Would Qantas support a recommendation from this committee that suggested to the government that it was illegal to impersonate someone who wanted to fly domestically?

**Mr Jackson**—That is a very good question.

**CHAIR**—Maybe at some point the security at airports could conduct random identity checks for passengers.

**Mr Jackson**—My answer to that would be conditional. The principal approach would be yes. However, for unequivocal support for any recommendation like that, we obviously would need to understand the accountability framework and the enforcement regime. The fact is that for a matter to be prescribed as an offence under law, even for us as an airline to contemplate going down the path of identity verification, we do not have access to Australian government—

**CHAIR**—I was not thinking about a sanction against the carrier; I was thinking about the individual.

**Mr Jackson**—I think my answer would still apply. For us to support that or for us to play a role in that, we would need to have a far greater strength and ability on a daily basis to access data that resides in government agency databases. Our databases are not intelligence databases,

which is why some of the frustration comes to the top from the police about why it takes so long to establish whether Steve Jackson or Stephen Jackson or Stephen John Jackson is travelling. That is because we do not have an intelligence database.

**CHAIR**—But when we have heard law enforcement agencies give evidence before us, both on the record and privately, the advice is that there is no sanction against known criminals being able to impersonate people and travel, particularly, as I made the point, being a drug courier from Perth to Sydney and then back if they do not catch them with the drugs in their possession. Wouldn't it just be another string to the bow to give authorities the opportunity to deal with people who are abusing the domestic travel situation?

**Mr Jackson**—Yes, certainly. That is absolutely correct. There is no sanction against individuals. I think if that sanction were available, obviously it would be up to agencies concerned to apply that as a tactical tool. They may choose not to, from a tactical perspective. But, yes, in principle, Qantas would support a recommendation of along the lines that you have suggested but with the qualifications that I have previously given you.

**CHAIR**—On the Aviation Security Identification Cards, you have amended the original submission from 180 credited to 76 actuals—

**Mr Jackson**—Sixty-seven.

**CHAIR**—Is that still too many in your opinion?

**Mr Jackson**—Yes.

**CHAIR**—Do you believe that there should be one single agency issuing ASICs?

**Mr Jackson**—In an ideal world, yes.

**CHAIR**—Do you know that we were at a port—and I think this was given privately, so I will not name the port—where we had a plane spotter who wanted to take pictures of aeroplanes landing. He applied for an ASIC at that particular airport. He was refused an ASIC at that port. Then he applied in Sydney and he was given one and next time the airport security—indeed, another ex law enforcement officer—saw him out there taking pictures of planes landing. That is not satisfactory, to my way of thinking. Have you come across instances of this yourself, where people at, say, Sydney Airport have been knocked back for a card and have gone elsewhere? You are an issuing agent, aren't you?

**Mr Jackson**—Yes, we are.

**CHAIR**—There are people who have gone down to Adelaide or Darwin and got a card—

**Senator MASON**—Card shopping!

**CHAIR**—Yes. It is card watch!

**Mr Jackson**—The short answer to your question is no. I cannot cite any specific examples. But I am certainly aware, to be accurate, of this in reference to the Visitor Identification Card, VIC, as opposed to ASIC. The system just simply would not permit anybody to walk into an airport and be issued with an ASIC. However, a VIC is a slightly different issue. The reason why Qantas are unequivocally supporting the government and OTS in their push to strengthen the VIC regime is to address those very issues. I will be unequivocal in this. There are some people who use the VIC regime to step around the ASIC regime. Mainly, in my experience, that is from being lazy, but it still does present an environment that those who might want to engage in criminal behaviour could exploit. That is why we are absolutely behind the government in strengthening the regime and moving to a significant reduction in ASIC-issuing bodies—and likewise with the Visitor Identification Card regime. There are amendments underway for the VIC regime to be strengthened quite considerably, which we fully support.

**CHAIR**—One in particular that TWU has raised with Qantas and the committee has been an issue. Of course, I must declare again and that I am a life member of the TWU. Particularly around security officers—particularly in Sydney—there is not the actual scrutiny of those people, overwhelmingly men, who are scrutinising people who come on to the air side. Not only has this publicly been raised but one of my Liberal colleagues from New South Wales has a whole list of security officers with Middle Eastern surnames. He is not here to say what he said about that, but these people are not necessarily scrutinised when they are scrutinising people who go into the airport. These issues have been raised with Qantas industrially. What is your response to the fact that you may have a situation where, because of laziness, as you say, or it just happens because you need someone on that shift for eight hours and Billy cannot do it, so you have got someone else to deal with it and they have a vehicle and some other formal identification or have none at all?

**Mr Jackson**—For any location where Qantas is the screening authority—and we are the screening authority at 26 terminals around the country—as I said in my supplementary submission, we subcontract three major security providers. My answer would be a categorical rebuttal of any contention made that—

**CHAIR**—Sorry to interrupt you, Mr Jackson, but I would like you to include this in your answer. As I understand it, you contract your security to three firms but they then subcontract that off to a number of other firms, don't they?

**Mr Jackson**—No, they do not.

**CHAIR**—They have, haven't they?

**Mr Jackson**—The only time that we would permit subcontracting under contract is if the primary contractor—which would be ISS, MSS or SNP Security—sought our permission to do so. They have in the past sought our permission and we have denied that permission. I want to be very clear and say that there are no subcontracted security officials on any Qantas location in any airport in Australia. How do we satisfy ourselves? Mr Bramah is the accountable manager for ensuring our internal assurance and audit regime, which works with the business and often the regulator to ensure that the requirements of both internal policy and the regulations are applied.

We often do no-notice and short-notice spot checks. If a contractor was found—and we have not found one—to be subcontracting without our knowledge then they would be placing their very commercially attractive contract in serious jeopardy. We are quite uncompromising on this front for the very reason that the TWU and other interlocutors cite as being an exposure to aviation security. We simply will not contemplate it.

**CHAIR**—There is the well publicised case of Gate Gourmet. I presume all of those employees who were charged in relation to that case had ASICs. We have been told that because of convenience—again not by some sort of deliberate policy—you will find people who go out and, say, take the catering on or off the aircraft or go and clean the aircraft are not all necessarily people who have been issued with ASICs. Gate Gourmet is a contractor to you. Are the cleaners direct employees of Qantas, say at Sydney?

**Mr Jackson**—Some are labour hire.

**CHAIR**—But the direct employees, I am sure, would probably have ASICs. Your instructions to your contractors are that they would have to. But we have had evidence given to us that, particularly on, say, the trucks going out to the aircraft, the only person who has got the card is the driver.

**Mr Jackson**—Nobody has ever placed any information before me in relation to that. We have specifics enough for it to be investigated if they were. We have said on public record numerous times, particularly to Mr Sheldon—and I will let OTS speak for themselves in terms of their position on this as well, which is very similar—that if you present information rather than making wide suggestions then our business is to receive specific information that will be aggressively investigated, and if it is found to be a breach of policy then the appropriate action will be taken. But I would have to say, in providing a full answer—and I alluded to this in my supplementary statement—that we apply the same rigorous background checking regime to our contractors as we do to our permanent employees. The argument that you can achieve a better outcome by simply having permanent employees only working airside—

**CHAIR**—I was not suggesting that. I was suggesting that it is probably easier to make sure that you have permanent employees with ASICs. Does Gate Gourmet still have the contract at Sydney airport?

**Mr Jackson**—Yes.

**CHAIR**—And you said you did a rigorous search of the employees who work for contractors. I am not sure if those were the words you used.

**Mr Jackson**—I am not able to provide you with specific information in relation to Gate Gourmet because the responsible business unit is Qantas Catering. But in the direct example cited by the TWU in evidence in relation to security officers on airport, as I previously said, we apply the same background checking whether they are contractors or whether they are direct staff.

**CHAIR**—So even though you represent Qantas you cannot speak for Qantas Catering.

**Mr Jackson**—In fairness to my colleague in charge of catering I would need to take that question on notice.

**CHAIR**—I am not being silly here—is there a separate security area for Qantas Catering there?

**Mr Jackson**—We provide the upper limit in terms of our expectations under our Transport Security Program, which gives effect to the regulations and the law, and we then hold the business accountable for how they deliver against that TSP through our audit program, as does the regulator through their own audits. My officers are not themselves personally responsible for delivering the security outcomes for Qantas—Q Catering.

**CHAIR**—Just so I understand, and my colleagues may correct me if I am wrong, as far as the fellows involved in the operation of Gate Gourmet are concerned, if Qantas Catering was as thorough as you are, Mr Jackson, they may not have been able to get a start there.

**Mr Jackson**—I would not be in a position to answer that.

**CHAIR**—I understand that.

**Mr Bramah**—Just a point of clarification: Gate Gourmet is a separate entity.

**CHAIR**—I know. Mr Jackson said that the company as a rule checks out its contractors and employees as well. That is all I am saying, Mr Bramah.

**Mr Bramah**—Yes, I see.

**Senator MASON**—Mr Jackson, your submission enthusiastically touches upon information sharing. What is the current process? What information do you share with other agencies at the moment?

**Mr Jackson**—I would like to provide a generic answer to that question, and then I feel that I need to make a request at a particular point to go into camera to give you some live examples.

**CHAIR**—If you would like to go into camera now, Mr Jackson, you can.

**Mr Jackson**—In terms of the generic answer, as long as we operate within the bounds of the law in terms of our compliance with privacy legislation and the agencies comply with their own respective secrecy provisions, my instruction to my staff is that they are to provide full and unfettered access to whatever information is requested.

**Senator MASON**—Is that when those agencies—government agencies; the Australian Federal Police, the Crime Commission and so forth—request the information, or is it when you take the initiative to give them certain information? They are different things, aren't they?

**Mr Jackson**—They are different things.

**Senator MASON**—Or both?

**Mr Jackson**—I have some very useful examples, so I think it is time to go into camera, and I would be very open in terms of those examples.

**CHAIR**—Okay. Do you want to ask anything on the record before we go into camera? I assume that once we go in camera that will be your day, Mr Jackson, and we will finish then.

**Mr HAYES**—There is just one thing. The Corby case brought extraordinary attention onto your baggage handlers. I know that the actual baggage line is run by the airport operator, but there are your personnel and it brought attention onto your baggage handlers. Since that occurred, I also note that Qantas has proceeded with a policy to casualise a lot of its labour, particularly in baggage handling. How much added security risk does that impose, and how much burden to you as head of security, in terms of Qantas?

**Mr Jackson**—I would suggest it adds no additional security risk, for the very reason that we apply the same security expectations of the business whether they engage labour hire or direct employees. The same rules apply, so it adds no additional burden to me at all.

**Mr HAYES**—Everyone who comes in, permanent or casual, would all be ASIC holders? Or do they get VIC passes?

**Mr Jackson**—That is (a) the regulation and (b) my policy. However, I cannot speak for the business. I am aware that there would be occasions—I cannot give you a specific example, but I am certainly aware that there would be occasions—of a labour hire worker, for example, who had not yet received the full background check and was therefore not entitled to an ASIC at that time. I am certainly aware that there is the opportunity for the business to perhaps apply my policy in a less robust way than I would like. My expectations and my security veto, given to me by the CEO, are uncompromising. If we find out that that has occurred, the business manager is held accountable. I am certainly not going to say to you that that does not occur. The VIC regime is there exactly as it is for a visitor, not to prop up a person currently seeking an ASIC. I need to be fair and say that absolutely that opportunity would exist, which is why we unequivocally support any measure to strengthen the process. It is double-edged. The process then for me internally with the business is that I really do need to put my black hat on and hold the business accountable if they let us down, because I am the accountable manager.

**Mr HAYES**—There is one other thing before we go into camera. It has been raised in the course of the hearings that some would wish to tighten up both the ASIC and MSIC regimes to greater ensure that the holder of the card is the person who is supposedly the holder of the card. Would you support greater verification of ASICs in terms of biometric application?

**Mr Jackson**—Yes, I would. I think we could talk for many hours about the pros and cons of biometrics, what it means to you and what it means to me, but certainly any innovation that goes to establishing identity—particularly where we have a process that not only permits you to work in a particular area but, as the Qantas card does, also gives you access through our embedded technology. My key performance indicator is very simple. I want to make sure that only those people that are entitled to go into secure areas go into secure areas. If biometrics provides us an additional benefit to enhance that then I would support it.

**CHAIR**—We will go into camera now.



*Evidence was then taken in camera but later resumed in public—*

[11.39 am]

**DREEZER, Mr Steve, General Manager, Maritime, Identity and Surface Security Branch, Office of Transport Security, Department of Infrastructure and Transport**

**RETTER, Mr Paul Bernard, Executive Director, Office of Transport Security, Department of Infrastructure and Transport**

**ROBERTSON, Mr Peter, General Manager, Aviation Security Branch, Office of Transport Security, Department of Infrastructure and Transport**

**ROWE, Mr Michael, Acting General Manager, Transport Security Operations, Office of Transport Security, Department of Infrastructure and Transport**

**WILSON, Mr Andrew, Deputy Secretary, Department of Infrastructure and Transport**

**CHAIR**—Welcome. I invite you to make a brief opening statement, which will be followed by questions from the committee.

**Mr Wilson**—I do not have an opening statement. I am just here to answer questions for you.

**CHAIR**—The committee understands that there are instances of people using visitor identity cards repeatedly to gain access to controlled areas as a way of avoiding the need to apply for MSICs or ASICs. What comments do you have on that and why has this practice not been stopped, particularly on ports?

**Mr Retter**—On the issue of visitor identity cards, I can first talk about the aviation sector. The government announced in the aviation white paper response that we would include additional measures to enhance visitor processes so that there were greater controls on who had access. Those arrangements have been the subject of extensive negotiation and consultation with industry since they were announced. I am pleased to report that the proposed arrangements are currently with the minister for his concurrence. Presuming that he is happy with those enhanced arrangements, we anticipate they will be issued in 2011. With regards to maritime, whilst there is no visitor identity card system similar to that in the aviation system, industry participants at ports are responsible for visitor control arrangements and the escorting and supervision of visitors on ports.

**CHAIR**—The Office of Transport Security is the body that credits people who issue the cards, is that correct?

**Mr Retter**—Are you talking about MSICs and ASICs in this particular case?

**CHAIR**—Yes.

**Mr Retter**—We oversee the policy arrangements that pertain to both the ASICs and MSICs, that is correct. As part of that we do appoint, subject to clarification, the issuing bodies that are the decentralised face of that regime.

**CHAIR**—Do you have it before you how many bodies are able to issue cards for maritime and airports?

**Mr Retter**—In the case of the maritime sector, there are approximately 22 to 23 issuing bodies. In the case of aviation, the current number stands at about 183. I would make the point, again as part of the aviation white paper announced by the government, that the minister announced that we would be moving to a series of enhancements to the ASIC regime, including a substantive reduction in the number of those issuing bodies.

**CHAIR**—We had an instance at an airport we went to where a plane spotter wanted to go onto the air site and take photographs of planes. He went to that particular airport for an ASIC and was refused one. He then—I will use my words—rode off to Sydney and was given one. The next time the airport security people saw the photographer was when he was out there taking pictures of planes. In light of what you are saying about the information you have given the minister, will that situation be able to be prevented?

**Mr Retter**—I would have to check the precise circumstances of the incident you describe, but my recollection is that in the incident at Adelaide—

**CHAIR**—That is the airport we are talking about.

**Mr Retter**—They made a decision that there was no operational need for that particular individual to receive a card. I am not familiar with the circumstances at Sydney Airport and I will need to take that on notice.

**CHAIR**—We were advised that he got a card because he just wrote off or went to Sydney airport and got a card from one of the 180-odd authorities there who could accredit him.

**Mr Retter**—The issue of whether he had an operational need from that airport's perspective is an interesting issue which I will investigate and come back to you on. I make the point that, notwithstanding your concern about whether he has an operational need to receive a card, he has to go through a background check. That background check is consistent—

**CHAIR**—He clearly went through the process somewhere else, and then the next time they see him he is taking pictures of planes landing. I am not worried about a photographer whose passion is taking pictures of aeroplanes for his website. We would be more concerned about not only terrorism but also more, as this inquiry is focussed on, serious and organised criminal figures being able somehow or another to subvert a system where you have 183 accredited organisations being able to give you some sort of tick to get on an airport.

**Mr Wilson**—As Mr Retter indicated, we will take the particular circumstances associated with the case you have raised on notice and provide information to the committee in regard to how that process operated and as to what operational reasons the individual provided to the issuing body to justify the issuing of an ASIC card. As Mr Retter indicated, that person will have

gone through the same background checking process that all individuals that receive an ASIC card go through.

**Senator MASON**—The point is the criteria are being differentially applied. We do not know, but that is the implication.

**Mr Retter**—I understand the implication—

**CHAIR**—Of course it is good that the security at Adelaide airport picked this up.

**Mr Wilson**—There are two points within the question. One goes to the operational requirements associated with the individual applying for the card, which is as far as I can ascertain from what you have said is the reason Adelaide airport refused to process the application for an ASIC. The second is that, having been accepted within the system to be processed, the individual has met the requirements of the background checking that is required to obtain an ASIC. As I have indicated, we are not in a position to provide information in regard to why the issuing body believed that there was an operational requirement for this individual to have the card, and we will provide you with information in regard to that.

**CHAIR**—Is it correct that the department commissioned a report from GHD Consulting regarding the eligibility criteria for ASIC and MSIC?

**Mr Wilson**—That is correct.

**CHAIR**—What has been the department's response to the recommendations made in that consulting report?

**Mr Dreezer**—The GHD report was part of an extensive departmental review of the Maritime Security Identification Card with industry stakeholders and government agencies. On 29 January, following that extensive review, the Minister for Infrastructure and Transport announced a number of arrangements to strengthen the MSIC scheme. I will go through those. The first phase of those enhancements came into effect on 1 July. Changes included increasing the number of offences that may preclude a person from eligibility for an MSIC. They more than doubled the number of offences, adding offences such as espionage, kidnapping, threats of violence, murder, fraud and dishonesty offences.

The second phase of enhancements came into effect on 1 December 2010. Those enhancements included a reduction in the maximum validity period of an MSIC from five years to four years, with an additional background check occurring at the two-year mark. Effectively that means that MSIC applicants may choose to have a two-year MSIC with a single background check or a four-year MSIC with two background checks. There were also penalty provisions placed in the regulations for MSIC holders who fail to disclose convictions of maritime security relevant offences.

Provisions were also put into the regulations enabling the prosecution of issuing bodies where they fail to cancel a card for a person who has been convicted of, and sentenced to a term of imprisonment for, a maritime security relevant offence. A further provision was added to the regulations to enable the secretary to suspend an MSIC under certain circumstances where a

holder is convicted of a maritime security relevant offence and, while not yet sentenced for that offence, is deemed to present a threat to maritime security.

**Mr HAYES**—That is only for when they have been convicted and not yet charged?

**Mr Dreezer**—It is for when they have been convicted and not yet sentenced for an offence. The department is working closely with our government partners and industry stakeholders to implement those measures.

**CHAIR**—Do the offences precluding eligibility include firearms offences?

**Mr Dreezer**—Yes.

**CHAIR**—Firearm offences preclude eligibility for the maritime card. Do firearms offences preclude eligibility for an ASIC as well?

**Mr Dreezer**—There are now a range of firearm offences included within the MSIC scheme criteria.

**CHAIR**—I asked about ASIC.

**Senator MASON**—And ASIC? Both?

**Mr Dreezer**—I would have to check that.

**CHAIR**—Please come back to us on that.

**Senator MASON**—How about sentences of imprisonment? Does there have to be a sentence of imprisonment?

**Mr Dreezer**—With the MSIC, unless the offence is an offence for which you are automatically disqualified—and I can go through those individual offences if you would like me to—

**Senator MASON**—No, it is all right.

**Mr Dreezer**—then you have to have both a conviction and a term of imprisonment.

**Senator MASON**—A suspended sentence, then, does not count for the purposes of the issuing of a card?

**Mr Dreezer**—Sorry—a suspended sentence?

**Senator MASON**—Yes. That does not qualify as imprisonment, does it?

**Mr Dreezer**—No, if the courts sentence a person to a term of imprisonment but suspend that sentence, then that would still be a maritime security relevant offence which would make that person ineligible for a card.

**Senator MASON**—Sure, but if a term of imprisonment is not imposed then it does not count, does it?

**Mr Dreezer**—If a term of imprisonment is not imposed, no.

**Senator MASON**—That does not mean it is not a serious offence, though, does it?

**Mr Dreezer**—If a person is convicted of a maritime security relevant offence and sentenced to a term of imprisonment but does not serve that term of imprisonment, they would still be considered to be ineligible for a card.

**Senator MASON**—I understand that distinction. That is just with MSIC—you do not know about the airport card?

**Mr Dreezer**—The same applies for ASICs as well, but I will need to check the firearms offences

**Senator MASON**—I asked this question before to another witness: how about offences contrary to the new serious criminal organisation legislation, such as anti-bikie legislation. Are they now part of it?

**Mr Dreezer**—I would have to check that as well

**Senator MASON**—You do not know? They are pretty important questions, are they not?

**Mr Wilson**—If I might, I do not believe that it is, but to be precise we will take it on notice and provide you with a precise answer.

**Senator MASON**—The report you have commissioned that the chairman has adverted your attention to concludes:

The current MSIC does not appear to be meeting policy objectives in that current eligibility criteria do not capture a range of offences and behaviours that are known to have linkages with terrorist activity and the unlawful interference with maritime transport and offshore facilities.

That is a big claim.

**Mr Wilson**—Since that report was made, the number of offences that are included within the scheme has more than doubled.

**Senator MASON**—I not even worried about the number. We are more concerned about the subject matter rather than the number. I don't really give a damn about the number.

**Mr Wilson**—As Mr Dreezer has indicated, they include issues such as espionage, kidnapping, threats of violence, murder, fraud and dishonesty.

**Senator MASON**—Yes, but you cannot tell me whether it includes offences contrary to the new serious criminal organisation legislation. You do not know.

**Mr Wilson**—Off the top of my head, I believe it does not but, as I have indicated, we will take it on notice to provide you with a precise answer because I would not want to mislead the committee based on my memory.

**Senator MASON**—Assuming your assumption is right, wouldn't you say it is a large hole?

**Mr Retter**—This goes to the heart of the purpose of the ASICs and the MSICs and the heart of the purpose of the appropriate acts—the Aviation Transport Security Act and the Maritime Transport and Offshore Facilities Security Act. Their purpose is primarily to ensure a more secure transport system for Australia. They are essentially focused on unlawful interference with vessels and aircraft and the range of activities that come under the definition of unlawful interference—taking control of an aircraft or vessel by force or threat of force or other forms of intimidation or trick or false pretence, destroying an aircraft or a vessel, causing damage to an aircraft or vessel that is in service and so on and so forth. My point is that the purpose of those two acts, when they were placed on the statutes and implemented, was primarily to deal with a terrorism threat, not a serious and organised crime issue. Our focus and the focus of the act and the associated regulations, including the various layers of security that we have in place as a preventive security regime in the aviation and maritime sectors, is about preventing unlawful interference in the context of terrorism. The issue that you raise, quite frankly, is an issue that I know has been debated—the policy position on whether or not the purpose of the acts should be changed. But that is a matter for government. We simply administer today's acts, and the purpose of those acts is not to deal with those matters.

**Senator MASON**—It is actually a matter for the parliament, not the government. The parliament will make a decision about that. You know the policy concern. I am just surprised that no-one there definitively knows the answer to that, because it is a pretty fair question to ask whether legislation relating to criminal organisations is included. I would have thought that was a very relevant aspect.

**Mr Dreezer**—It is AusCheck who makes a determination as to whether an individual offence fits within the eligibility criteria or conditions. What we need to do is approach AusCheck to make that determination.

**Senator MASON**—I am surprised you do not know this sort of thing. Obviously I am expecting too much.

**Mr HAYES**—Clearly this particular inquiry is about whether maritime and aviation security settings are right in combating serious and organised crime. I have no quarrel with your view that the genesis of both ASICs and, more recently, MSICs was about terrorism. The added offences for the exclusion from the issue of those cards do have an association with making assessments about crime itself.

Customs—and probably anyone else who deals in the space of serious and organised crime, particularly in relation to the importation of illicit substances and contraband—have been informing us that the area of most hazard for us is the ports. What I would like to know from your department is: have we got the settings right on transport security as it applies to ports? I am asking about not simply the category 1 designated ports of Sydney and Melbourne—they have their own issues there, I suppose—but across the board: we see great differences in port security, quite frankly.

**Mr Wilson**—As a department, we can only comment on our own piece of legislation. I am not comfortable—and nor would it be appropriate for me—to comment across the breadth of the AFP, Customs and any other agency that may or may not be involved in the overall security settings within the ports. In that sense—

**CHAIR**—But you must be a member of some sort of joint body that coordinates, aren't you?

**Mr Wilson**—Yes, but I would not be any more comfortable with the AFP, Customs or any other agency proffering opinions on my part of government operations than I would be in proffering opinions on theirs. I am not a trained police officer. I am not a trained Customs officer. We do work across portfolios but, in terms of the areas of responsibility of this portfolio, I am comfortable with the settings that we have in place. They can always be improved and, as Mr Dreezer indicated before, we are going through a process of improvement within the MSIC and ASIC regimes, and we are going through improvements in our relationships with the operators on ports and airports, in terms of their transport security plans. In that sense, it is a continuous journey of improvement. But, as to the settings that the government has asked the portfolio to administer, I am comfortable that we are administering them in accordance with the legislation.

**Mr HAYES**—I simply thought that, in the light of your submission—where you say that the need to strike a balance is reflected in the risk based approach of OTS which continuously enhances security in Australian transport systems—you may have had a view on that and not be simply relying on the view of Customs, AFP and everyone else in the process.

**Mr Wilson**—And we do. We seek information from our partners at ports and airports and from stakeholders within government and external to it as to the arrangements that we have in place under our pieces of legislation and the arrangements that industry or others put in place. So we constantly work with our stakeholders and partners within government to improve the systems. But there is always a balance in terms of how rigid or structured the arrangements may be, and the need to facilitate the transport task and the capacity of people to work within that transport task. Not to put too fine a point on it, it is the job of the minister and parliament to make those balanced choices. We provide advice to the minister on that, and he and the parliament make choices as to the end outcome.

**Mr HAYES**—Given that Customs say that the maritime environment poses the highest risk in relation to the importation of prohibited goods into Australia, does the Office of Transport Security maintain, have or monitor customs brokers at all—freight forwarders—who work adjacent to the actual port infrastructure?



**Mr Wilson**—If I might, I will ask Mr Retter to answer the specific question that you have asked. The initial comment in regard to Customs is on importation—I would take it, importation of products that are—

**Mr HAYES**—Illicit.

**Mr Wilson**—illicit, as opposed to focused on maritime security issues. So—as far as I can read it—they are coming at it from a different point of view from us. But I will ask Mr Retter and Mr Dreezer to answer the specific question.

**Mr Retter**—Our focus, and it flows from the purpose of the act, is on the ship to shore interface. At a port we focus on the actions of port facility operators, stevedores and port service providers. We do not have a focus on whole of supply chain in the maritime sector, which is where you are going, as I understand it.

**Mr HAYES**—So the Office of Transport Security has solely a regulatory function then?

**Mr Retter**—We are a preventive security regulator. We influence the settings of that regulatory approach based upon a very clear understanding of what the threat is with an absolute focus on terrorism. We work very closely with the Australian intelligence community as a whole and ASIO in particular.

We work through a very careful process of looking at high-risk locations and what needs to be done. We adopt an approach which says essentially that one size does not fit all. Each port and airport has different vulnerabilities that need to be addressed differently. What works, for example, at Port of Sydney may not work at Melbourne Ports Corporation. I can give you quite explicit examples. My point here is that the regulatory settings and how they applied on the ground at each port and airport which is regulated by us do differ not so much in the nature of the layers of security that might be in place and the culture and training that accompanies that but because the infrastructure and the challenges at each of those ports is different. The degree of risk associated with a terrorist type activity or an act of unlawful interference will vary depending upon the nature of the port and airport.

**Mr HAYES**—For the Office of Transport Security to have greater regard in terms of serious and organised crime being perpetrated either through airports or maritime facilities, you are saying you would first need a change in policy setting?

**Mr Wilson**—Our task is not serious and organised crime. That is very clear within our legislation. We are a regulator of the transport network in terms of a security outcome. Just as the Civil Aviation Safety Authority is a regulator of the aviation system in terms of the safety of its operations, we are akin to it in terms of security operations. We are not a regulator of serious and organised crime.

**CHAIR**—No, but you have actually mentioned terrorism about five or six times as an issue, which is understandable, but you have only just mentioned now serious and organised crime.

**Mr Wilson**—I was answering Mr Hayes's question in terms of—

**CHAIR**—I am not having a go at you, Mr Wilson; I am just saying that that is the emphasis on what all these are—

**Mr Wilson**—That is the emphasis of our legislation. The ASICs and MSICs are established under our legislation. Our legislation is about threats to the aviation and maritime environment in regards to countering terrorism. It is not in regards to serious and organised crime. That was a decision of the parliament in establishing that legislation. Does that answer your question, Mr Hayes?

**CHAIR**—Are we able to get a copy of the accredited issue of cards?

**Mr Wilson**—The list of organisations that are accredited to issue cards?

**CHAIR**—Yes, if that could be supplied to the committee. You said on airside there are 183 accredited bodies that issue cards but actually only 67 that do issue cards. Why is that?

**Mr Retter**—The changes that have occurred since the ASIC arrangements came into place are such that, for many of the issuing bodies which originally applied to become issuing bodies, it became economically not feasible because of the numbers involved. We saw a natural progression to a smaller number actually being responsible for more cards being issued—in other words, we saw dominant players setting up in certain regions and, if you like, taking over that function. Indeed, some of the smaller issuing bodies essentially subcontracted to the bigger ones to do the job.

**CHAIR**—So there are 116 who do not use their powers; you are going to take their accreditation—

**Mr Retter**—From memory, of the 183, I think the figure is in the forties who currently issue a card—

**Mr Dreezer**—Approximately.

**Mr Retter**—As I indicated before, as part of the announcements in terms of improvements and enhancements to the regime, as announced by the government, it is intended to reduce the number of card-issuing bodies to a smaller number. That process will unfold as part of the range of implementation initiatives already announced under the white paper. The intention clearly is to look, first of all, as a first step, at those who voluntarily no longer wish to be an issuing body. I suspect a lot of those who are no longer actively involved in issuing cards see no benefit in that process and would like to be removed. We are hoping that in a voluntary sense we would see a number of those disappear and then thereafter we will make some decisions about exactly how many issuing bodies would be an appropriate regime.

I will make two points about that. In essence, it is a bit similar to how you get a passport around Australia by going to a post office and filling out a form and then sending in your application, which is then centrally dealt with by bodies here in Canberra, by DFAT, who make the assessment. What we see with our issuing bodies around Australia is essentially a decentralised geographical approach to make it easier for the workers at our ports and airports to put in the application, to then have an initial assessment done in terms of: does this person work

at the port, do they need unescorted access to secure areas at ports or airports? That form is then sent off to a centralised body through AusCheck, which is our centralised coordinator through the Attorney-General's department in terms of the background-checking process, which is the key engine room, if you like, of the whole deal. That is where the consistency of the process and the robustness of the process exist. We have one agency responsible for a decision about who gets or does not get a card in the first instance and thereafter, assuming it is a green light—'Yes, that person has passed the background check'—permission is sent back to say, 'Yes, individual A, B and C may get a card.' We essentially have a decentralised acceptance of application and issue of a card, but a centralised decision making here through AusCheck and Attorney-General's, which then obviously work with the agencies which have to provide the elements of the background check.

**Senator MASON**—Do you have significant liaison with overseas ports and airports to try to determine where world's best practice for security is?

**Mr Retter**—There are a couple of levels: firstly, in terms of the regulators of many of the nations that Australia deals with both in a maritime and an aviation sense we have quite strong links, obviously, in those areas where you would expect us to have which are closer to Australia or where there is a strong trading arrangement or routes in terms of passenger numbers flying. In a separate layer we conduct on a cooperative basis, and often on a reciprocal basis, inspections of regimes, particularly given the threat levels in the aviation sector where we look at the robustness of the aviation requirements as articulated in annex 17 of the ICAO requirements, which are the international settings.

**Senator MASON**—The international covenants.

**Mr Retter**—Yes. Basically, what we are trying to do is to work with those countries to ensure that what is expected internationally is being put in place and, if there are instances where we think something needs to be improved, we then sit down and work with that particular nation, that regulator and the industry participants there to actually do some capacity building to address it.

**Senator MASON**—That's good. I understand.

**CHAIR**—How much is the application form to fill out for ASIC and MSIC? Is it \$500?

**Mr Retter**—I might refer that to Mr Dreezer.

**Mr Wilson**—Just to add to Senator Mason's question, we also have international exposure in our participation in the International Maritime Organisation and ICAO in terms of the future settings concerning aviation and maritime security.

**Senator MASON**—Obviously Australia plays a leading role in that, Mr Wilson? Is that right?

**Mr Wilson**—I think we try to punch above our weight. We have a fairly healthy reputation in both of those organisations.

**CHAIR**—Do you have the answer, Mr Dreezer?

**Mr Dreezer**—The cost of an ASIC card is between \$180 and \$200—that is the commercial charge that covers the card application and issue. For the MSIC, the current cost is around \$240 for a two-year card and approximately \$460 for the four-year card. Those are both commercial charge costs.

**CHAIR**—Why is it \$180 to \$200 for an ASIC card? Why the difference? Why wouldn't it be just the one figure?

**Mr Dreezer**—Because they are commercial charges. The only constant in those charges is the AusCheck charge for production of the background check process. For ASIC that is \$81 for the ASIO and Crimcheck process. For MSIC that is \$81 as well for a two-year card. For a four-year card—because there is obviously an additional background check—AusCheck charge \$160 for the four-year card check. There is also an additional \$4 should there be requirement for an immigration check. But the charges for ASICs and MSICs are a matter for the commercial entities.

**CHAIR**—Is more scrutiny applied for a four-year card than for a two-year card?

**Mr Dreezer**—For a four-year card there are two background checks, which require two sets of input into those background checks. Therefore there are larger administrative costs.

**CHAIR**—There is more scrutiny of somebody who wants to work for four years rather than two?

**Mr Dreezer**—No, it is just that at a two-year interval, instead of reapplying and getting a new card, you can have the same card but there will be behind the scenes a background check done at the two-year point. It is exactly the same in terms of the background checking arrangement.

**Senator MASON**—It is the same integrity for both cards?

**Mr Dreezer**—Correct.

**CHAIR**—Thank you very much, gentlemen, for coming along.

**Proceedings suspended from 12.17 pm to 1.00 pm**

**JOHNSON, Mr Jeremy, Business Manager, Biometrics, CrimTrac**

**KENNETT, Ms Roberta, National Manager, Background Checking Services, CrimTrac**

**SMITH, Mr Douglas, Chief Executive Officer, CrimTrac**

**van GESSEL, Ms Theresa, Manager, Policy and Legal, CrimTrac**

**CHAIR**—I welcome officers of CrimTrac. I invite you to make a brief opening statement, which will be followed by questions from the committee.

**Mr Smith**—I would like to thank the committee for the opportunity to appear today to answer questions concerning CrimTrac's submission. Since taking up the role of Chief Executive Officer of CrimTrac, I have been committed to supporting a very clearly stated national vision for information sharing that provides police and other law enforcement officers with the tools to keep Australia's community safe through rapid access to useful information. I am committed to ensuring that CrimTrac is able to deliver on the national vision through sustainable funding and resourcing that recognises, supports and enhances the national value of the services that CrimTrac provides.

CrimTrac's responsibilities in providing police with rapid access to national information have expanded since it was established in 2000. This has occurred as technology has advanced and as communities have become increasingly mobile. At the same time, the expectations of the nation that law enforcement will proactively address issues such as terrorism, have a national view on organised criminal activity and use advances in technology to address these issues have also increased. The increased expectations for security of the nation will require a focus on sustainable solutions for the future.

The submission that CrimTrac made in 2009 outlined some of the possible solutions that could assist law enforcement in the future. Since the time that submission was made, CrimTrac has completed the second phase of a feasibility study into national case management. The CrimTrac board of management has endorsed CrimTrac conducting an investigation into the privacy, legal and economic issues associated with the creation of a national investigative management system. A national investigative management system would provide police and law enforcement officers with an information and intelligence sharing mechanism to manage serious organised criminal activity and terrorist related activity across the country.

CrimTrac is currently investigating these issues with the aim of providing a clear business case to the CrimTrac board. If I may, I will just caveat responses here today with the information that while I believe that I have a very good understanding of CrimTrac's activities and the issues that would concern this committee. I would seek your indulgence and just point out that I have only been in the position of the CEO for four weeks today and I may defer questions to my colleagues.

**CHAIR**—Regarding the national case management system you said that the study was concluded.

**Mr Smith**—A feasibility study into the National Information Management System was presented to the board at the December meeting in 2010. A range of operational issues, financial issues and a number of operational issues that have been given back to us to have a look at arose. We have a responsibility to report back to the board at their meeting in March.

**CHAIR**—Are you able to chair with the committee any of the findings of the study?

**Mr Smith**—It is probably a little bit early and perhaps unwise to go into the details of every aspect of the study. However the first point about the study to put on the record is that there is an absolute benefit to the nation and to national law enforcement and to the activities related to organised crime and investigation of terrorism activity in having a National Information System and a National Case Management System. The advocacy for that and the arguments for that are incredibly strong. The issues surrounding the actual form that the system would take are quite complex because you are dealing with the jurisdictional issues where everyone has a different method of doing business, and these have been canvassed many times before in many places.

The issue, however, is that, firstly, the system should have absolute benefit and absolute support amongst all of the jurisdictions, and this is outlined in the commitments given at places like the board of management. Once we resolve, if you like, the contribution issues and how it would be finally designed into an operational form we can then get into the stage of putting forward a business case.

**CHAIR**—For the record, in your submission you recommend that consideration be given to the use of automated number plate recognition capability at all ports and airports. Could you outline to the committee why you think that is important.

**Mr Smith**—With a range of identifying tools like ANPR we are talking about tracking movement into and out of secure areas at ports and airports. The purpose is twofold: to ensure that we know who has come in and out of the secure areas airside of the airport or at the port and, also, by extension it creates a capability that can be preventative and investigative. You have the ability to automatically record what vehicles have come in and that then gives you the possibility of having alerts for flagging at-risk vehicles or vehicles of interest.

**CHAIR**—You submit that a single National Case Management System would increase investigation and efficiency. Would you like to explain on the record why you think that would assist efficiency?

**Mr Smith**—The two elements are efficiency and effectiveness. When it comes to effectiveness, having a single source of the truth in an investigative endeavour is absolutely critical. From an effectiveness point of view it means all people involved in a particular investigative effort can go to the one place to find out what activities are being done by all participants in an investigation. From the point of view of efficiency, the reduction of inefficiency with a single system is that you do not have people with multiple points of data entry and you do not have the different and often contrary business practices that can sometimes work against the effective investigation. In financial terms, it means you do it once and you do it right.

**Senator MASON**—CrimTrac’s primary role is to provide national information sharing solutions to support the effective operation of police services and law enforcement agencies across borders. We heard some evidence from Qantas. They are keen to better develop a relationship and share information among law enforcement agencies. Does your brief potentially include private companies, or do you really only look across government agencies?

**Mr Smith**—The mandate that is given to CrimTrac comes from an intergovernmental agreement which was first signed back in 2000. That is, if you like, the contract that brings together the various jurisdictions. The short answer to your question is that we have no mandate to deal with private companies. If we were to deal with private companies in providing that sort of capability, there are a whole raft of privacy, legislative and other practical issues that would have to be negotiated.

**Senator MASON**—It sounds like Mr Jackson and Qantas are going to have to do their and work with the law enforcement agencies. Anyway, I think they appreciate that. You have recommended the inclusion of biometric markers on the MSIC and the ASIC. Is that because you believe that is the most efficacious unique personal identifier? Is that your point?

**Mr Smith**—The reason for the recommendation is that you are trying to address vulnerabilities. You are trying to address the core issue in providing secure perimeters and proper access to places like airports and ports. If you look at the mischief that the ASIC and the MSIC attempt to address, it is about who is coming into the airport or the secure area at the port. Our recommendation is aimed at enhancing the treatment you apply to the vulnerability, that being the perimeter of either the airport or the port. The better that you eliminate the potential for misuse, checking or—

**Senator MASON**—Card swapping or lending or whatever.

**Mr Smith**—Yes. At the end of the day it is about who is coming into the airport and whether they are an at-risk person. Therefore, the better you check the person who has got the card, the more you reduce the vulnerability at the border.

**Senator MASON**—The technology is readily available to ensure that biometric markers are a system with significant utility, isn’t it?

**Mr Smith**—I may defer to my colleague Mr Johnson. When we do about things being readily available—

**Senator MASON**—At a price, no doubt.

**Mr Smith**—I was just going to caution that there is always a cost and there is always a deployment issue. In addition, there are privacy and other issues with respect to the security of the data that you are collecting. So the practicality and the possibility should not be confused with the legislative and policy issues. I will defer to Mr Johnson on the actual practicality of that.

**Mr Johnson**—The technology certainly exists to capture and store biometrics on a card and link it to a person with a device or a database.

**Senator MASON**—With biometrics, what unique identifier would you look at?

**Mr Johnson**—Certainly from CrimTrac’s perspective and a law enforcement perspective, we have a long-established database of fingerprints. Although CrimTrac does not currently run a facial recognition system, facial recognition is growing in popularity, and that is used in some law enforcement agencies and certainly the Passports Office. That is also a proven biometric technology.

**Senator MASON**—You are right to be cautious about the privacy aspects. Those of us who have been around a while would remember in 1987 the Australia code debate and, in more recent years, the social security facilitation code—the access code. Even more recently, there was the health card. The issues always are: who has access, what information is held, and so forth. It is a huge issue when it is to be given to 22 million Australians but perhaps slightly less significant in some ways when you give it to a particular group of people for a particular purpose. The issues are still there but perhaps without the same privacy concerns. They are still there but perhaps they are somewhat less astringent, if I can put it that way. If you could have a card with biometric information on it, would you seek to include other information? The technology is there to include all sorts of information. Would that be part of the proposal?

**Mr Smith**—Implied in your question is: what sort of biometric information could be used to enhance security and, therefore, reduce vulnerabilities with respect to people accessing an airport? I think it is rather trite to say that the technology is there to add a whole raft of information. It is not just about the card. One could potentially speculate about a whole range of different methods of access to secure places, but the question that has been put to us is with respect to a card. It is the position of CrimTrac that the use of biometric data—in particular, fingerprints, which is the readily available technology—would enhance the validity of the card, the checking of the person and therefore go some way to addressing some of the vulnerabilities at the crossing point into secure areas at airports and ports.

**Ms van Gessel**—Perhaps I could clarify one aspect. The submission that CrimTrac made did not necessarily recommend that biometrics be included in the physical cards themselves. That is a different aspect that, of course, can be explored. Our main contention was around the background checking of the person, when you are conducting a criminal history check. We submit that it would be useful to consider conducting a fingerprint check at the same time to ensure that the identity of the person who is presenting themselves is in fact the person who is presenting themselves. It overcomes some of the vulnerabilities in the system, such as names not being matched correctly or documents that have been obtained fraudulently being verified as valid. That was the main thrust of our initial submission. The secondary aspect is to look at the inclusion of a biometric for controlling access to and from the site. So there are two aspects to it. Perhaps if we could clarify which of the aspects we are talking about, that might help us to provide you with more accurate answers to your questions.

**Senator MASON**—The technology is there have those sorts of cards and make it more specific. I am sure you could do this. You could make the card available for use in certain parts of an airport or a port—in other words, the card can be made quite sophisticated, can’t it?

**Mr Johnson**—I think that can be done irrespective of—



**Senator MASON**—It can be done.

**Mr Johnson**—biometric or not. Even swipe cards that we all carry for access—you can program them to access one room and not another.

**Senator MASON**—Exactly. Thank you.

**Mr HAYES**—Firstly, congratulations, Mr Smith, on your appointment. You have taken over an organisation which is held in very high regard in this place. It is certainly an organisation that has a very significant effect on contemporary law enforcement.

**Mr Smith**—On both points, thank you, Mr Hayes.

**Mr HAYES**—Is the national police case management system likely to replace the existing state system, such as PROMIS or COPS—PROMIS in the Northern Territory, where you are from.

**Mr Smith**—I think it would be a very ambitious agenda for me to start to address the possibilities downstream. The specific brief that was given to CrimTrac was to look at the specific requirements that came out of Justice Street's inquiry into the Haneef case—the review by Mr Roger Beale—and at the recommendations that the NCTC, the National Counter-Terrorism Committee, had before it, and then come up with some proposals on national case management. If we could talk about capability rather than system, I think we would get a better understanding of what we are talking about. When one talks about systems one tends to look at the physical infrastructure—how the computer may look—but it is probably more desirable in a discussion such as this to talk about capability. We are talking about the capability of all jurisdictions to participate in an investigative tool that has greater efficiency and effectiveness. I really would be brave to forecast the outcome and how that may end up years from now. As a vision, and this is my personal view, I believe it would be ideal to work towards commonality—interoperability in the capability that all jurisdictions share with their investigations. But that is a very adventurous and visionary thing to be discussing at the moment. Our specific task that we were given by the board of CrimTrac and the NCTC was to investigate the investigative capability, the national case management capability, and to address the specific issues that were before them, which included interoperability, if you like, with respect to counterterrorism investigations.

**Mr HAYES**—Do you also think the MSIC and ASIC cards would have some role in a national police management system—recording that information as well, or not recording it but having access directly to it?

**Mr Smith**—There are a raft of issues here, and I would have to defer to my colleagues as to the actual process today. The policy issues have implications for privacy—for data storage and the purposes of data storage. When we talk about the actual checking that is being undertaken, there are policy implications about holding the data with respect to who the applicants are, how long that can be held for and the purposes that it can be held for. As advised at the moment, there is no connection being proposed with the ASIC check for the purposes of providing information back to AusCheck on the suitability of the person—they are the ones who make that decision, not CrimTrac. So there are the questions of the purpose of the gathering of the information, the

storage and the privacy rules with respect to that storage, but I will defer to Ms Kennett to go further in that.

**Ms Kennett**—CrimTrac's role in the ASIC and MSIC process is that we provide a criminal history background check to AusCheck to contribute to their decision-making processes. There have been some conversations around some of the vulnerabilities of name based checking. Some of those have already been mentioned, but, essentially, it is possible for people to change their names and there are complications around matching with names. We need to use a fuzzy logic algorithm to allow us to match names that have, perhaps, been misspelt or are in a different order, or things like that. There have been some early discussions around strengthening that name based checking regime and using biometrics as an identifier to help strengthen that regime.

**Mr HAYES**—If that became part of the regulation, you would simply check the fingerprint on the application against the national fingerprint database?

**Ms Kennett**—There are a number of different ways that it could be done, but that would certainly be one of the options we would explore.

**Mr HAYES**—Would that be a way of ensuring at least that the applicant is the person who they are making the application for and, secondly, of making sure that the applicant does not have an assumed identity to cover up offences that they have already been prosecuted for?

**Ms Kennett**—It would certainly allow us to confirm the identity of the individual. As far as the criminal history aspect is concerned, as long as the assumed name or any other information was linked to that original identity those would be exposed as well.

**Mr Smith**—Mr Hayes, I would like to add to my earlier answer. Regarding the issues about the holding of the information on the applicants of the ASIC and the MSIC, if it were accepted as a matter of policy that CrimTrac would, for example, do continuous checking based on parameters that were provided, there would of course be a necessity to have access to that information on a continuous basis; that is implicit in the ability. By extension, you would then need to deal with the issue of who has access to that data. As we have said in our submission, we recommend that there be an ability to enhance the security of airports and seaports to address vulnerabilities with respect to identities and that there be continuous checking. In answer to one of the terms of reference of this committee, once you have that you then have the capability for information sharing to take place. Implicit in that, there are then the questions of privacy, the rules of access and what the information can be used for. Our recommendation, which is on page 5 of our submission, is that some consideration be given to that capability. But of course once we start that discussion we then need to have the discussion about the purposes for keeping information—the continuity of checks, the frequency of the checks and all the questions that come with that.

**Mr HAYES**—With the sort of information that you inevitably hold, and will hold if we proceed down this path, would you then see it as appropriate to consider CrimTrac and its personalities subject to the same integrity regime of the Australian Crime Commission—or the Australian Federal Police, for that matter?

**Mr Smith**—With respect to the issues of integrity, the checking of our people is at the highest levels of the public service standards at the moment. One thing I need to make clear is that the access our people have to the actual data is quite restricted. CrimTrac is the facilitator of capability, as opposed to the decision maker with respect to various law enforcement holdings. I just need to make that clear, because as a facilitator I think nearly all of our people—I would have to take advice on this—have very limited, if any, access to any ‘live’ data, as we call it. That is not the function of CrimTrac; that is for the various pods of access.

**Mr HAYES**—I understand that.

**Mr Smith**—With respect to the standards of integrity, of course the more involved CrimTrac becomes in holding what one could call ‘operational’ data, then of course it is definitely a discussion that needs to be had and some policy decisions taken. I have absolutely no problem with considering the highest standards that any committee may recommend in that regard.

**Mr HAYES**—It is just that, if we are moving in the direction where on an ongoing basis you are holding very sensitive information, I think you would be silly to not think that we would have to address issues of checks and balances as they apply there. I know that in the AFP those integrity standards exist not only for sworn police officers but for administrative support as well. The more this goes in that direction, it would be highly likely that we would have to consider a higher integrity regime being imposed on CrimTrac.

**Mr Smith**—I have absolutely no problem with that. I can recall reading somewhere in my briefings that CrimTrac has conceded that having the Law Enforcement Integrity Commissioner responsible for overseeing integrity standards in CrimTrac was an acceptable proposition. But I might defer to Ms van Gessel on that point.

**Ms van Gessel**—Certainly we have made submissions in the past that, should the decision be made, we would have no difficulty with CrimTrac falling under the remit of the Australian Law Enforcement Integrity Commissioner. At the same time, the submission has also been made that at this stage there have been no questions raised about the integrity, for the reasons that Mr Smith has outlined—our staff do not have access to the information, we are not inputting information, we are not retrieving information and we are not manipulating information. So, while there are some potentials for vulnerabilities, those potentials are very minor compared to those in law enforcement operational agencies such as the Crime Commission or the Federal Police. However, we would have no objection should that decision be made; it would fit within the overall security and privacy regime that we already have in place.

**Senator MASON**—Do you access the information?

**Ms van Gessel**—Personally, no. I do not think any of us at the table have access to information. The only time access to information is granted to anyone within the agency is for the specific purpose of checking, when there is a problem with the system. When the police ring up to say, ‘Look, this image isn’t coming up’ or ‘This record isn’t coming up’, we have testers. But there are auditing records and monitoring procedures in place around that access. If someone rings up and asks: ‘What do you know about Senator Mason?’ we cannot look you up, you will be relieved to know.

**CHAIR**—Anything you need to know about him, just ask us. As there are no further questions, thank you very much for coming along today. It is very much appreciated.

[1.31 pm]

**LANGTON, Mr Kim, Managing Partner, Australia Pacific Region, Chameleon Associates (Australia) Pty Ltd**

**CHAIR**—Welcome, Mr Langton. I invite you to make a brief opening statement, at the end of which members of the committee will ask you questions.

**Mr Langton**—Thank you. I am here because I bumped into Senator Hutchins at a border security conference last year. I had made a presentation on aviation security and what goes on in regard to the screeners, what goes on in the airports in general and how it runs. I have over 30 years experience in the security industry and for the last seven or eight I have been involved with Chameleon. We have been training aviation, specifically predictive profiling, for the AFP. We have trained over 300 AFP in the airports in Australia, New Zealand and overseas. I see some problems there and I brought those up at that meeting—that is why I am here.

**CHAIR**—In your view, are there any gaps in the current security processes at ports and airports? Do you think there is any weak link that should be brought before the committee that we should deal with? Do you have any suggestions?

**Mr Langton**—Yes, I think there are a number of issues. I do not think contract security is the way to go to run screeners. We are looking at the security of the country, not at a factory site out in Western Sydney where you can put a security company on. I am experienced in this; I have many, many years experience doing it. To run it properly you really need a model similar to what they have in New Zealand with Avsec—maybe TSA, but I think Avsec is the best model I have seen overseas.

As a contractor working for either the airport or the airlines, you have to remember the contractor has to make money. To do that means that the training he supplies and the level of service he supplies will not be as good as they would be if it were run by a government body. If you look at the airports at the moment and the civilian contractors that are there, your turnover is massive. They have major problems with sick days, people working double shifts and it has even got to the point with some of the contractors that we have subbies working for the contractors. I just do not think that is the way to go.

**CHAIR**—We specifically asked one of the airlines, Qantas, about this issue this morning. Qantas said they have three contractors involved in their security and none of them subcontract their contract work. That is what Qantas said; I am not saying that is the case for any of the other operators.

**Mr Langton**—I can tell you there are subcontractors working for contractors.

**CHAIR**—For Qantas?

**Mr Langton**—I cannot specifically say for Qantas, no.

**CHAIR**—A number of submissions have recommended that there should be a continuous background check and the use of fingerprints to improve ASIC cards. Do you have a view about those suggestions?

**Mr Langton**—I agree and I also agree with the last speakers that biometrics is the way to go. You really need to know where the card is going. I can take a card and, as long as I look similar to the person who is meant to have it, I can get in whereas with biometrics you are controlling access and egress of the site. Biometrics is the way to go.

**CHAIR**—Mr Langton, current airport and portside security measures have a counterterrorism focus. Do you believe that there is a need to expand this focus to include the prevention of serious and organised crime and would such a move, in your opinion, undermine existing counterterrorism measures?

**Mr Langton**—Most of the training that we do overseas is counterterrorism, but we can do the same training in, say, the Mall of America in Minnesota, in the US. The training that we give them for counterterrorism picks up all the bits underneath, because you are going for the highest common denominator if you are looking for terrorists. If you are looking at that level you will pick up all the bits underneath and that includes criminal activities. The methodology that a criminal uses, whether it be in major crime or shop theft, is pretty well the same as what you would get from a terrorist. The method of operation, the way that they pre-plan, the way they do dummy runs, the way they actually do the act and the way they get away are all very similar. If you look at a military operation, it is very similar to the way that a terrorist operates. You are looking at one to five years to plan it and you are looking at the method that he uses and how he gets away. If you were to use a level of security that is up to catching terrorists, I believe you would be quite capable of picking up all the crime that goes on underneath.

**CHAIR**—From its inquiry so far, the committee has noted the important role played by trusted insiders in criminal activities. From your experience, what proportion of border related crime involves trusted insiders?

**Mr Langton**—I can not give you a figure but I can give you an example. We run training exercises with the AFP, New Zealand Police and Avsec. As part of the exercises, we turn them into terrorists. We train them to think like a terrorist. We then flip them to become security. If they already know how to be a terrorist, it gives them a different way of looking at it from a security point of view. Part of that exercise is to sit them down and ask them to plan an attack—it could be of an airport, the Opera House, anything. We sit them down for an hour after, say, our first day's training, and they have to put together a feasible plan of attack for that protected environment. I would say nine times out of 10, when everyone puts together their plan, there is an insider. Whether it is someone who is in security or a cleaner who is gathering intel or doing observations for them, there is always someone inside. That is because the people that do the job—security, police—understand that if you are going to get information that is the best way to get it.

**CHAIR**—One issue that has continued to be of interest in our inquiry is the use of criminal intelligence and how far that should go in determining someone's eligibility for cards, employment et cetera. Your background is in predictive profiling. Can you go into a little bit of detail for the committee about how your professional pursuit might assist law-enforcement

agencies in determining what sort of person should or should not be eligible for consideration of cards, employment, promotion et cetera?

**Mr Langton**—We use predictive profiling for HR, mainly in the States. All you are really doing is looking at a method. If you are looking at employing someone, you do your normal background checks. You look at where the person has come from, you look at their employment history and from that you can build up a pattern. You can also build up a picture of that person, and by using that you can basically tell how they are going to react in certain circumstances. I am not talking about doing psychoanalytic tests on them, but you can read them. You can tell where they come from, their background and you can put a risk level on it.

**Senator MASON**—Because the best predictor of future behaviour is past behaviour. Is that what you mean?

**Mr Langton**—Yes.

**Senator MASON**—This morning we heard from the chairman's friends in the Maritime Union and they made a claim on the issue of profiling. There is a recommendation to the committee in a report by Dr Nolan from the ANU, and the report has been endorsed by the union.

**CHAIR**—They got him to write it.

**Senator MASON**—Indeed, they paid him to write it. This is recommendation 9 of Dr Nolan's report, on page 10:

Consider the discriminatory impact and human rights violations caused by the MSIC scheme if ethnic or other profiling based on individual, social or demographic characteristics is to be used.

Individual, social or demographic characteristics—are they aspects of appropriate personal profiling?

**Mr Langton**—No, race is irrelevant.

**Senator MASON**—Sure. What about individual, social or demographic characteristics?

**Mr Langton**—No, they are irrelevant too.

**Senator MASON**—So they are not the characteristics that you would look at anyway?

**Mr Langton**—If you were profiling a person as they were coming up to buy their ticket, the first thing you would do is look at that person as a whole.

**Senator MASON**—Their behaviour?

**Mr Langton**—Everything—how they are carrying their bag, all that sort of thing. You would then ask them a few questions, and security questioning is different to police or intelligence questioning. The questions are very general, but you would be able to put together a picture of

that person based on the sorts of answers you get. I will give you a perfect example: Anne-Marie Murphy. I do not know if any of you are familiar with her. She was a pregnant Irish woman who in the late 1970s tried to board an El Al flight at Heathrow airport. She was about seven months pregnant, had red hair, was Catholic and was travelling alone, going to Ben Gurion airport. When she got there, you would think it is a bit odd that a woman who is Irish Catholic and very pregnant is going to Israel—

**Senator MASON**—Travelling by herself.

**Mr Langton**—by herself. When she was pulled over and questioned by El Al security, they were asking her general questions: ‘Why are you going there?’ She said she was going to the holy places. She did not have enough money. She did not have the right sorts of credit cards to verify where she was going. She had no place to stay. They immediately thought, as you would probably think, that there was something odd about it—plus, where she was going to stay in Israel was in Bethlehem at the Hilton. There is none.

**Senator MASON**—No, there is not.

**CHAIR**—Senator Mason has been to most of the Hiltons.

**Senator MASON**—There is certainly one in Tel Aviv.

**Mr Langton**—There is, yes, on the water. But the security guard doing the profiling put it together that this woman was either doing surveillance or she was a mule, because it did not fit. Why would a woman who is pregnant be going to Israel? They checked her baggage—which, I might add, had already been through all the technical checks—just by holding it up to see what weight it was and it seemed too heavy. There was 2.6 kilograms of Semtex in the bottom of the bag. She was picked up by profiling, by looking at her and how she was pregnant. The story she gave did not fit.

**Senator MASON**—It just did not make sense?

**Mr Langton**—Yes. The profiler was saying, ‘This is wrong,’ and he automatically thought that she was either picking up intelligence or a mule. As it turned out, she had been picked up by a Syrian tourist. He had got her pregnant. He had told her that he wanted her to go home and meet his family on the West Bank. He was a Muslim. He did not want to travel with her because ‘something had come up’. She was not to tell the Israelis that she was going there to marry a Muslim because they would give her a hard time. He put her on the plane to basically blow up herself, 300 other people and the aircraft.

**CHAIR**—So she did not know it was in her suitcase?

**Mr Langton**—She did not know. She was totally oblivious to the whole plan. She now has a 21-year-old son. She lives back in Ireland, and the Syrian who did it is still in jail in London. That is one of the real success stories of profiling. She had been through all the technology.

**Senator MASON**—That is through the X-ray machines and—



**Mr Langton**—She had gone through everything. You have to remember with technology—and I think our reliance on technology is far too great; we ought to bring back the human element—if there is an X-ray machine that they are using at the airports and you are dealing with state sponsored terrorists who have a lot of money, what is to stop them from buying that same machine, pulling it apart, working out what works and what does not work and then setting their plan to it? The only thing they cannot count on is a security guard coming up to them and asking them a question, because they do not know what they are going to get asked. That is where profiling and questioning come into it. It adds an error that the terrorist just cannot cope with. It can work exactly the same for someone who is going in and doing a test run to steal some clothes from Kmart. Security guards are already on the defensive. It is Israeli based security but it works.

**CHAIR**—That is something that is terrorism related. How would it work for something that is criminally related? I know that your expertise is in airports, but how would that work for, say, a port?

**Mr Langton**—Exactly the same. You would be looking at the crew. You can profile manifests. You could even look at where the ships have been. The AFP and Customs do it now.

**CHAIR**—So something might be that they are a very poorly paid crew or—

**Mr Langton**—Yes. If you have two people going on an aircraft and one of them is a middle-aged businessman who flies business class and is a frequent flier and one is a 19-year-old who comes from the back of Mogadishu who has a one-way ticket, which one are you going to question? You would question both, but to the first one you would probably say, ‘Thank you, sir. Have a nice trip.’ The second one it would be worth having another look at.

**Senator MASON**—I will ask you in private later on, Mr Langton, why I am always stopped. I do not know why I am always stopped, but I always am.

**Mr Langton**—If I could suggest anything to the committee it would be having a look at the way they do it in New Zealand. The Avsec model works. It is because their employment system is under one umbrella. They all work for the government. They have the same uniform. They have the same intelligence structure. They have the same training. They all get paid very well. If you look at what they do at Avsec in regards to employment and turnover, you will see that they have no turnover. You almost cannot get a job in Avsec. You compare that to what goes on at our reports with our contract security where it is a revolving door. That cannot be good for the security of the airport.

**CHAIR**—One of the things we have come across and which has privately been said to us—particularly by the airport corporations, not so much by flyers—is that the advent of the Jetstars and Virgin Blues and the price of an airline ticket now as opposed to what it was 20 years ago has meant that cost pressures on airlines are just enormous now. The growth in the international terminals means now it is almost like going into Myer or David Jones.

**Mr Langton**—We have an opportunity at the moment with the AFP, because they are going through this process where they are removing their protective service officers, PSOs. They are giving them the choice that they can either join the AFP as an AFP officer, if they can pass

muster, or in reality be out of job. We have this very, very well-trained aviation related security force that is sitting there at the moment that will become redundant over the next year or so. I just think that it is criminal that these guys, who are very well trained and very motivated, will be basically put on the scrap heap. I have seen at the airports we have gone to and all the training we have done with the AFP that usually half the class are PSOs, sometimes even three-quarters. They are worried they are not going to have a job because they know they will not pass the tests that are involved to become an AFP agent. But they are very good security guards. They are much the best. Yet we are going to lose that experience because of the removal of the PSOs. If I was running it, I would create an Avsec and I would utilise those guys as the backbone of my Avsec. Then everything would be run under the same intelligence, the same training, at good pay and with a good career structure. Then the problems we have in regard to screeners and security at airports would disappear.

**CHAIR**—Mr Langton, thank you very much for coming along today. There being no further questions, I would like to thank all our witnesses for their time and effort in attending today's hearing.

**Committee adjourned at 1.52 pm**