



COMMONWEALTH OF AUSTRALIA

# Official Committee Hansard

JOINT COMMITTEE ON THE AUSTRALIAN CRIME  
COMMISSION

**Reference: Annual report 2003-04**

THURSDAY, 17 MARCH 2005

CANBERRA

BY AUTHORITY OF THE PARLIAMENT



## **INTERNET**

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

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

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

**JOINT STATUTORY COMMITTEE ON THE  
AUSTRALIAN CRIME COMMISSION**

**Thursday, 17 March 2005**

**Members:** Senator Santoro (*Chair*), Mr Kerr (*Deputy Chair*), Senators Denman, Ferris, Greig, Hutchins and Mr Byrne, Mrs Gash, Mr Richardson and Mr Wood

**Members in attendance:** Senator Santoro and Mr Byrne, Mr Kerr, Mr Richardson and Mr Wood

**Terms of reference for the inquiry:**

To inquire into and report on:

Australian Crime Commission annual report 2003-04

**WITNESSES**

**BRADY, Mr Peter, Senior Legal Adviser, Australian Crime Commission ..... 1**  
**MILROY, Mr Alistair, Chief Executive Officer, Australian Crime Commission..... 1**  
**NEWMAN Mr Lionel, Director, Executive Services, Australian Crime Commission..... 1**  
**OUTRAM, Mr Michael, Director, National Operations, Australian Crime Commission ..... 1**  
**PHELAN, Mr Andrew, Director, Corporate Services, Australian Crime Commission ..... 1**  
**POPE, Mr Jeff, General Manager, National Intelligence Services, Australian Crime Commission..... 1**



**Committee met at 6.06 p.m.**

**BRADY, Mr Peter, Senior Legal Adviser, Australian Crime Commission**

**MILROY, Mr Alistair, Chief Executive Officer, Australian Crime Commission**

**NEWMAN Mr Lionel, Director, Executive Services, Australian Crime Commission**

**OUTRAM, Mr Michael, Director, National Operations, Australian Crime Commission**

**PHELAN, Mr Andrew, Director, Corporate Services, Australian Crime Commission**

**POPE, Mr Jeff, General Manager, National Intelligence Services, Australian Crime Commission**

**CHAIR**—I declare open this public meeting of the Parliamentary Joint Committee on the Australian Crime Commission. Tonight's public hearing is on the committee's inquiry into the annual report of the Australian Crime Commission. The report covers the first full reporting year of the commission's operation. I would like to welcome the ACC's Chief Executive Officer, Mr Alistair Milroy; its Director, Executive Services, Mr Lionel Newman; its Director, Corporate Services, Mr Andrew Phelan; its Director, National Operations, Mr Michael Outram; its General Manager, National Intelligence Services, Mr Jeff Pope; and its Senior Legal Adviser, Mr Peter Brady. For the information of witnesses, the committee prefers all evidence to be given in public but, should you at any time wish to give your evidence, part of your evidence or answers to specific questions in camera, you may make application to do so and the committee will give consideration to your application. However, evidence taken in camera may subsequently be made public by order of the Senate or this committee. The usual practice of the chair is to call on the chief executive, as in this case, to make an opening statement. Would you like to do that, Mr Milroy?

**Mr Milroy**—Yes, Chair. This is the first full year report on the outputs and activities of the Australian Crime Commission since its establishment on 1 January 2003. In the past two years I believe the Australian Crime Commission has made significant inroads into achieving its goal of reducing the incidence and impact of serious organised criminal activity. The ACC has delivered actionable criminal intelligence and significant intelligence assessments to assist its partner law enforcement agencies with their investigations and also to enhance their knowledge of specific areas of criminality. Based on intelligence submitted by the ACC following board approval, we have successfully conducted special investigations and intelligence operations in partnership with Commonwealth, state and territory police services and other law enforcement agencies in order to protect the Australian community from the impact of serious organised crime. The ACC places a significant amount of emphasis on the need for stakeholder partnerships in conducting its various areas under the menu of work.

The 2003-04 report outlines the activities of the ACC, and I will touch on some of the highlights. We have disrupted and dismantled a number of criminal groups. These include firearms manufacturing and distribution groups, drug importation groups and groups involved in the distribution of drugs, and also those involved in money laundering. I can indicate that in the two years to today's date the Australian Crime Commission have disrupted 27 such syndicates.

We have provided over 700 operational disseminations to law enforcement agencies and government and foreign agencies. If the committee wishes, I can provide a brief outline of some of those disseminations and the bodies which received them. In the reporting period we have conducted 355 examinations and issued 453 production notices using our coercive powers. We have restrained \$16 million in proceeds of crime, forfeited \$2.4 million and issued \$19 million in tax assessments.

From 115 drug seizures we have recovered 1.7 tonnes of drugs and precursors, including the largest seizure of pseudoephedrine in Australia—some 750 kilos. We have seized 3,552 firearms and components. We have charged 203 persons on 626 charges. If the committee desires it, I can relate those activities to the current achievements to date as a comparison.

We have also endeavoured to show how our intelligence operations and investigations have extended to affect the criminal environment through law and administrative reform proposals and the benefits from cooperation with the wider law enforcement community. All ACC operational activities are underpinned by intelligence and strategic use of coercive powers. The ACC has continued to focus on building a skilled work force to deliver high-quality, integrated services. The ACC is committed to evolving its menu of work as the dynamic criminal environment changes and the priorities of its stakeholders change. We have sought feedback on the usefulness of the intelligence products supplied and we have also surveyed to a great extent our stakeholders to find out what they require in relation to intelligence and also to pursue the attack on organised crime.

We will continue to work to dismantle and disrupt criminal syndicates under this partnership model and enhance Australian law enforcement capacity by targeting the high-threat serious and organised crime groups that we have been identifying with our partners through a picture of criminality process. Through this value-added intelligence cycle to Australian law enforcement, the ACC aims to be recognised as a leading provider of effective intelligence and investigative capability. The ACC has also undertaken initiatives to enhance law enforcement coordination by conducting joint agency and industry intelligence probes, improving the nature of intelligence collection mechanisms and establishing joint management processes within all jurisdictions to target serious and organised crime.

I acknowledge that the committee raised a number of concerns in respect of the 2002-03 annual report covering the ACC's first six months. These include aspects of ACC business planning and performance measurement, criminal intelligence services, operations and investigations and timeliness. I believe that the ACC, in producing the 2003-04 report, has addressed the majority of these concerns. This report reflects the ACC's continuous improvement processes. I am confident that the ACC will be reporting further significant successes in the 2004-05 report and we will continue to improve our processes and maintain high-level governance management accountability and mechanisms. An example of that is the development of the effectiveness and efficiency framework to complement the ACC's current extensive outputs and activity reporting process. I look forward to receiving the committee's report. I thank you for the opportunity to make this presentation.

**CHAIR**—Thank you very much for your statement and the report. It is probably useful to proceed by asking questions at least initially about the three main outputs that are detailed within the report. I will refer initially to output 1.1, Criminal intelligence services. As the report



indicates, in an overall sense there has been an increase in activity for this output since the last report. Is there any particular reason for this other than the fact that the last report reported partly on the ACC and partly on its predecessor, the NCA, whose activities were curtailed in the last month of its existence?

**Mr Milroy**—Your question is in relation to why there has been an increase in activity?

**CHAIR**—That is correct.

**Mr Milroy**—I think that has a lot to do with the approach that the ACC is undertaking in terms of its intelligence collection and identifying those areas that are required to be targeted in partnership with our various stakeholders.

**CHAIR**—You are saying that the increase in activity goes beyond the simple mechanical curtailment of the NCA?

**Mr Milroy**—I think that it has a lot to do with the focus that the ACC is undertaking. There is a far more comprehensive approach to intelligence collection and the analysis of such intelligence which has given us a more enhanced understanding of crime in the Australian community. Mr Pope could probably provide a more detailed answer, if you wish.

**CHAIR**—Would you like to add to that, Mr Pope?

**Mr Pope**—The only things that I would like to add would be that I was advised—I was not there at the time—that since the middle of last year we have increased our staff, particularly within a strategic criminal intelligence area. That naturally translates to an increase in output. We have also improved our processes and that results in an increase in output. I would like to think that we are more focused with respect to our intelligence priorities and, therefore, are working towards more articulated and clear goals for our board agencies.

**CHAIR**—There is an interesting reference on page 31 of the annual report where you note that the database ALEIN is a secure national extranet which is used by, among others, a large number of government law enforcement agencies. Further, in 2003-04, 1,580 new users self-registered to ALEIN. With such a large number of people entitled to view and contribute to the material, how is it possible to keep the site and its information secure? Is it the same secure process for the database called ACID?

**Mr Phelan**—You are talking about ALEIN or ACID?

**CHAIR**—No, ALEIN, given the big increase in users.

**Mr Phelan**—ALEIN is the network which provides communications to allow users to access ACID. The security within ACID is clearly to a highly protected level.

**CHAIR**—Could you just elaborate on that? There is an interlink between ALEIN and ACID, is there?

**Mr Phelan**—Yes.

**CHAIR**—Where is the information contained?

**Mr Phelan**—There is some information in ALEIN at the present time. I will just go through some of the details of what ALEIN is. It is really an interface for delivering certain systems to the users, the users in this case being a number of law enforcement agencies across Australia and New Zealand, including of course the ACC. The specific database within that is ACID, the Australian Criminal Intelligence Database, so that you go in through ALEIN to access ACID. There is also another database called ViCLAS, which is the Violent Crime Linkage Analysis System, which you also access via ALEIN. Even though ALEIN is essentially a communications system it also contains a range of information. Within ACID you tend to have unsorted intelligence reports. ALEIN can sometimes contain value adding reports provided by various users, which are sorted according to certain desks which have been created within ALEIN. Without getting too technical, within ALEIN you can have different levels of access depending on your need to access certain of those desks and the information contained in them. The desks, for example, can include certain national security aspects but generally nothing within ALEIN would exceed 'highly protected', which is not the highest non-national security classification level. Does that answer your question? To get into ACID you need to access ALEIN. ALEIN would give you access to ACID. There are certain ways of logging access and there are certain access limitations within ACID itself but also within ALEIN.

**Mr KERR**—I suppose the words that trigger our interest are 'self-registered'—new users are 'self-registered'—which implies that there is a process which quite a large number of people are entering. I suppose the obvious concern is: how do ACC, and presumably other agencies, control that entry point?

**Mr Phelan**—With great difficulty, I would have to say. We have a risk management framework around ACID and ALEIN, so we do declare the minimum standards that we expect for people who are able to access ACID. But in a shared information source, which ACID is, where we are relying on the quality of information provided by our partners out there in law enforcement agencies, we obviously need to take a risk in terms of who is accessing it. We rely on the agencies concerned to essentially ensure that only those who are properly accredited to do so can access their systems.

**Mr KERR**—Does it have a back-checking system so that every keystroke for entry is recorded so you can do random spot checks, audits and the like?

**Mr Phelan**—Yes, we can audit access to ACID.

**Mr KERR**—And you do?

**Mr Phelan**—We do.

**Mr WOOD**—It is true that the users of ACID have all taken ASIO checks?

**Mr Phelan**—I could not say that, no.

**Mr WOOD**—I am just going from what I have heard.

**Mr Phelan**—I doubt it very much. To do an ASIO test would probably require a level of clearance that is not common around police forces, so in general terms I would say no. But amongst the Commonwealth agencies I would expect that, if people had been cleared to the level of highly protected, for example, there would have been a vetting process to put them to that level, which may include an ASIO test.

**Mr WOOD**—Just from my own experience, that would be the same for the level of protected—you would have an ASIO check undertaken. The question I have is with regard to how to improve intelligence and name identification across Australia. The area I am very interested in is the way police forces or law enforcement agencies across Australia work fairly much in isolation. I believe there is a strong need to connect those. What are your thoughts on that?

**Mr Phelan**—The board of the ACC has recognised the importance of law enforcement agencies across Australia and New Zealand in contributing to the overall national criminal intelligence, so it has set up what is called the information-sharing working group, of which I am the chair. The terms of reference of that group are really to understand the legal, physical, technical and other—dare I say it, cultural—impediments that might prevent law enforcement agencies from providing intelligence reports into ACID, which is the national criminal intelligence database. So the objective there is to really understand what the problems are and to come up with solutions cooperatively with our partners to achieve that aim. At the present time, yes, there are significant stovepipes within various law enforcement agencies across Australia that prevent a complete or comprehensive provision of intelligence into the national database.

**Mr WOOD**—That would not just stop the intelligence—it is also for name identification, for example. What are your thoughts on agencies not having automatic access to those who may have explosives licences, for example?

**Mr Phelan**—Obviously, there are a range of privacy issues. The history of databases in Australia really reflects legislatures across Australia—all states and federally—coming up with information sources or databases to cover information specific to whatever is the purpose of the agency that owns it. So surrounding each of those databases will be a purposeful clause to do with privacy, the ability to access information and so on.

Very often, because the databases are for very specific agencies, they can be excellent—they can be very good—because the whole purpose of the agency clothing them is to support the provision of quality information. It is a very big issue for an agency set up for one particular purpose to be able to access the other databases, given the overall privacy legislation in Australia. Part of the role of the information-sharing working group is to help us identify what those databases are and what they are carrying so that we can purposefully work through each of them and understand how we can perhaps deal with any legislative, privacy or other reasons to encourage a maximisation of the provision of information to ACID itself.

**Mr WOOD**—Law enforcement agencies across Australia have access to find out whether a person has a motor vehicle registered in their name, a trailer registered in their name, a shooter's licence or a crowd controller's licence, but not an explosives licence. As I see it, law enforcement agencies need that information and it needs to be national so that, if a person

crosses from one state to the next, a law enforcement agency can easily undertake a check to find out that person's background. What are your thoughts on that proposal?

**Mr Milroy**—What I might mention here is that the whole purpose of the board establishing this information-sharing working group, which, as Andrew alluded to, in fact brings in a lot of agencies in addition to state police forces, is that through the board process there is the opportunity—to pick up on Mr Wood's comments—to refer issues for improvement through to the Australasian Police Ministers Council, as we have been doing with some of the issues that we have been uncovering in firearms. So that is where we need to take this, because you are talking about individual state jurisdictions and we are trying to bring all this together and advise the board on some appropriate resolutions. And that would pick up, I think, on the issue that you have raised—hopefully.

**Mr KERR**—Putting it in a 'higher order' context, two of the objects of the reporting are (1) to report on trends and the nature of crime threats and (2) to report on the law reform that is required. The point that Mr Wood raised, were it thought to be appropriate, would emerge as a recommendation for law reform and for allowing greater integration of access to these databases. Of course, parliamentary history is replete with some concern about that also, so the balancing consideration would emerge. In direct answer to what has been suggested, you have not yet proposed a law reform initiative in relation to the explosives register?

**Mr Milroy**—No.

**Mr BYRNE**—With respect to ALEIN and ACID users, I notice you have 12,756 users of the ALEIN system and 8,271 ACID users. I think about 2,313 documents were submitted through ALEIN and 128,718 intelligence and information reports through ACID. So it is clearly a system that is getting fairly extensive use. You have 1,500 new users of ALEIN and, I think, 574 new users of ACID. When does that system become clogged up? Are there any difficulties with this information system and accessing this system?

**Mr Phelan**—One of the important initiatives that the ACC is implementing is called ALERT. It has two parts. The first is to produce or buy hardware which enables a capability of nearly 24 hours a day, seven days a week and which does not fall over and can be backed up. We have not had that up until now; there was always a high risk associated with it. The second is to create hardware which is capable of carrying just about anything known to humanity. So, in terms of capacity under the ALERT initiative, there should be no issue whatsoever. In relation to the tools which the ALERT initiative is creating, they are to produce far greater analytical mapping information, being able to do what is called contextual searching, looking for trends that automatically alert analysts and allow feedback et cetera. That database really is hungry for as much information as possible. So we do not see any foreseeable limits in terms of the information carriage within it or in terms of user capability. Certainly, within the ACC we have taken infrastructure decisions in partnership with the Federal Police to create capacity to move data around as well.

**Mr BYRNE**—I notice you were smiling a bit. Have you had difficulties with the current systems? Was there some problem with hardware crashes or files being lost or anything like that?

**Mr Phelan**—No, we have been fairly lucky up until now—and I use that word advisedly. I think the system has performed fairly well, so the down time has not been great. But, increasingly, we have had to have scheduled down time, which may on occasions limit access at particular times of the year as we flush servers et cetera. We have had one incident which I think produced down time because of some corrupt code going back to whenever. We identified that within about 24 hours. As far as I am aware, the only down time that has exceeded nominal periods of an hour or so since I have been in the Crime Commission was that one time.

**Mr BYRNE**—Have you monitored any unauthorised access to this particular system at all? Have there been any incidences of that?

**Mr Phelan**—We certainly monitor. There can be no unauthorised access to the system. The system is quite robust. Getting back to the question asked by Mr Kerr, I think, earlier on, obviously we rely on our partner agencies to ensure that there is a regime. You can only access ALEIN via the systems that are possessed by, say, the New South Wales Police or Customs or whoever has access to it. People, to be in the building, to access their systems and therefore go in via ALEIN, need to have passwords and need to be qualified. We log the password access. It is impossible for there to be any hacking. I will not say ‘impossible’, but there is a very robust set of security measures to prevent this from occurring. It is an extranet and the whole of the cabling and everything else associated with it will prevent anyone digging a trench and tapping a wire into it right through to getting unauthorised access.

**Mr BYRNE**—Is the maintenance of the system outsourced or done in-house?

**Mr Phelan**—It is done in-house.

**CHAIR**—You are notified then by the various agencies as to who has been granted authority to access by that agency—names and logon numbers—and you are able to monitor that?

**Mr Phelan**—Yes. There is a central desk within the ACC which essentially releases and controls that access. It issues the passwords et cetera.

**CHAIR**—Are you satisfied that there have been no breaches since the system became operative in its current form?

**Mr Phelan**—I do not know who is at the other end of a wire. As far as I am aware, we have had no reported incidents of someone in another agency using any password. Mr Pope, are you aware of any?

**Mr Pope**—I am not aware of any reported unauthorised access, no.

**Mr BYRNE**—With respect to that, you could have someone access the system and then there is someone else in one of those agencies that might be leaning over and having a look at that. What are the precautions for that sort of stuff?

**Mr Phelan**—There is no defence against that, quite frankly. We reinforce with our partner agencies the sorts of behaviours that we expect of people who access our system, but we are reliant on those agencies policing it. It is an environment where the information, even though it

is Commonwealth information, really is shared information. It is a service; accordingly, we have to manage risks around that. We could clamp right down and we would get no information at all. So, to venture, we have to allow this sort of partnership model in the interests of encouraging the provision of quality intelligence.

**CHAIR**—I want to follow up a little more on that point, but I will go to Mr Richardson, who I think has some questions along this line of inquiry.

**Mr RICHARDSON**—Along the same lines, Mr Phelan, you said that you had conducted an audit in relation to the personnel who had access to either ALEIN or ACID. Was that done by a spot check two or three times over the annual report period? What were the rough dates that it was done? You have already answered my final question, which was: was there any misuse reported at this stage?

**Mr Phelan**—We police the audits for usage and we do spot checks back into the agencies. I cannot give you the dates but we routinely review on a regular basis logon IDs and passwords to see who has not accessed it. If someone has not accessed the system for a period of time—and I cannot recall what the time is—we will automatically shut that password down. So they need to positively revive and go through a trim-down process to do so. So we do have routine checks of that nature. There is no evidence of unauthorised use but we do know that people will leave agencies and the agencies may forget to tell us or people might move on and we will just cut that off and revive it later. But we do not regard that as misuse; that is just not fully informing us of what has happened.

**Mr RICHARDSON**—Is it a set group of personnel that always does the audit in a particular year?

**Mr Phelan**—Yes. The people who conduct the audit are within the ACC's IT area, so, yes, there is a dedicated group of people who administer ACID and ALEIN and ensure that access control is up to speed. Again, the policy and business rules are driven by the intelligence directory.

**CHAIR**—Just following up on the people who are given authority to access: are there any stated criteria provided by the ACC or have criteria been provided by the NCA prior to the establishment of the ACC so that there is a common set of criteria which enables a certain type of person or a certain level of officer to gain access to the system? In other words, do all the jurisdictions and the various agencies have set criteria?

**Mr Phelan**—They do, yes. I do not have them on me but I can certainly provide them for the committee, if you wish.

**CHAIR**—What sorts of things would be contained in the set of criteria that enable somebody to gain access and a password?

**Mr Phelan**—The need to know is one of the criteria. The agency would only authorise or allow someone to apply for a password who needed to access the information it contained or input information into ACID. We would obviously need to rely on that agency to self-regulate that within the partnership arrangements. We would normally also insist that the persons

concerned had been through whatever probity checks were relevant to the agency concerned. From recollection, we do not seek to impose a mandatory Commonwealth highly protected level, although that would be our ideal. There is some further work to be done in that area, particularly as we encourage more use of ACID as the ALERT program rolls out. So I would not say that the criteria are going to spell out the sorts of details that we do internally in the ACC in terms of access to our systems. There are certain standards put in broad terms where we are largely also reliant on goodwill. Some agencies use ACID as the only intelligence database but, interestingly, they tend to limit the users who can access it. There are differences as to how many people access input information through to how people access the information. Some have a more devolved and decentralised environment. Some have more centralised and tightly controlled environments as the throughput for ACID.

**CHAIR**—Are there any other questions that committee members want to ask in relation to output 1.1?

**Mr WOOD**—Is it correct that there is a log-out time if a person walks away from their computer?

**Mr Phelan**—In ALEIN itself it is a few minutes; I cannot recall just how much. It will certainly shut you down if there has been some inaction from a particular point in time.

**Mr WOOD**—Is it a stand-alone computer? Can you have a number of different projects on the one computer?

**Mr Phelan**—For example, in the ACC we access ALEIN through the Windows environment, so we can have a number of windows open.

**Mr RICHARDSON**—Are there any frustrations in relation to the intelligence-led policing model in conjunction with, say, the number of personnel that you would like to see go into that area to assist the ACC?

**Mr Phelan**—Sorry, I am not quite sure what—

**Mr WOOD**—I am just inquiring as to whether you believe you should have more personnel going into the intelligence arena of the ACC to facilitate a better policing method or a better policing-sharing method across the states.

**Mr Phelan**—I think we have an appropriate balance at this point in time. There is a lot of work on people's plates but we think the balance is there.

**Mr Milroy**—As part of this information-sharing working group, Mr Phelan is actually taking his experts to each jurisdiction to get an understanding of what stakeholders are currently using, and at the same time briefing them on the capabilities of the ACC systems and on the new ALERT initiative and the benefit that is to Australian law enforcement in particular. For example, Victoria are now going through a change of their systems and Queensland are too, so we are finding some jurisdictions can see the benefits of joining the ACC in a greater interface between their systems and our systems. So we are trying to work across jurisdictions to end up

with a far more advanced and more efficient national criminal intelligence database which will benefit not only the ACC but also our partner agencies.

**Mr RICHARDSON**—That is certainly what we wanted to hear.

**Mr Phelan**—One of the important things is that there are a lot of developments happening. A lot of the police forces across Australia are faced with a range of very expensive options to lift their game internally for intelligence. Through the ALERT initiative we can actually leverage a lot of the resources, which are perhaps people and information resources, to produce a better result. That is why we emphasise this partnership risk management approach to leverage those extra resources.

**Mr Milroy**—In actual fact the ALERT initiative is now in its third year of tied funding. In other words, tied funding is set on a certain program, we have programmers onboard and there is another 18 months to go under that process. We are starting to see some of the products now starting to roll out and also the benefits that Mr Phelan alluded to.

**Mr KERR**—I have a question about the intelligence area. Your report focuses on the strategic assessments you have made in the intelligence reports. One of the tasks that was explicit before and maybe implied now is threat assessment over the horizon. I suppose that would not only relate to your partnership arrangements with states but would perhaps also involve bringing in some inputs from overseas, the AFP and various other sources. That would enable you to report on emerging threats so that we position ourselves to be more ready, rather than get the information about what is actually in the last period of time. There is nothing mentioned about that in the report. There is the picture of criminality in Australia, which seems to be a snapshot or a descriptor of what the picture is, and there are a number of alerts about things that are on the immediate horizon. I am wondering whether any work is being done on that issue of anticipation so, I suppose, you, the AFP and other partner agencies can anticipate placing resources into particular areas rather than being overwhelmed and then catching up.

**Mr Milroy**—Yes. Before I ask Mr Pope to comment, I will just give you an indication of what the agency has been doing. When we first started we took a view, or a ‘clean sheet of paper’ approach, to building the intelligence directorate and we did not just accept what we inherited. In that process we looked in particular at one of the critical roles that we have to perform, and that is the over-the-horizon assessments and the strategic assessments. To that purpose we looked at the international framework that has existed—where we are going to collect the intelligence. The AFP have got certain parts of the world covered, as does Customs, and we looked at the gaps.

The director of intelligence and I went to the UK for discussions with the British over the new serious organised crime department they have been setting up, the National Criminal Intelligence Service. We had meetings with Europol about how they can contribute to an international collection framework through the AFP and, where we cannot do it through the AFP, about what other areas we can use to achieve the overall objective. We then dispatched the national intelligence director and an expert to a number of countries in Asia, not only to market what the ACC is about but also to look at the trends coming out of some of those regions which impact significantly on Australia.



Again we made contacts with a number of other law enforcement agencies, including in New Zealand. From that we have now developed, in consultation with the AFP, what you might call a global network of collection. An intelligence collection process has been developed by the ACC, which Jeff can brief you on. That has now gone out internationally to collect the intelligence that we are asking for, to pick up, as you pointed out, what the next threats are and how we can be one, three and five years ahead and advise government through the board. We have been putting out a number of strategic assessments at the moment but that is a very important part of our function—

**Mr KERR**—That is not picked up in this report, though, so presumably it is in next year's report.

**Mr Milroy**—That is right, and of course it is part of the process. This also feeds into the picture of criminality process which eventually the national threat assessments across the various crime types have produced. So it is the framework, but that feeds into that process. Jeff can probably expand a little bit more if you wish for further information.

**CHAIR**—Mr Milroy, before Mr Pope commences, I need to attend to an item of urgent business in the Senate, so I will hand the chair to Mr Kerr and I will be back in a few minutes.

**Mr Pope**—To add to what Mr Milroy has just mentioned to you, I think in many respects your observation of the report is correct. That is probably an accurate reflection of where the intelligence directorate was at the time of the report. Before we start looking over the horizon we really need to understand our environment now and we need to set up those collection processes and those sorts of relationships and set our intelligence products right. I mentioned earlier that we had staffing challenges around that same time.

I think you will find that this year the report will be vastly different in this area and I would like to briefly outline the areas where it will improve along this line. Last year the picture of criminality went out about three years to 2007 and this year the picture of criminality is going out five years to 2010. Late last year we committed to the board that we would produce a number of strategic criminal intelligence assessments throughout this year. We have already delivered the first one, being a major fraud probe. I believe we have about another 12 scheduled for this calendar year. They are on a variety of topics and they go out a minimum of five years and up to 10 years with respect to the topics included. We have also been setting up national threat assessment processes with our partners, if you like, to monitor the changes in serious and organised crime groups. So I think you will find a vast improvement in that area, given that our intelligence directorate is certainly moving forward quite rapidly.

**ACTING CHAIR (Mr Kerr)**—Let us move to output 1.2. One of the issues that seemed surprisingly innocuous in terms of the outcomes is the business regarding identity crime and card skimming. Whilst there were a number of seizures of quite large numbers of cards, the numbers reported do not seem to match the huge growth in phishing and all other electronic crime areas of identity fraud. I am wondering whether it is just historical, in the sense that you are coming late into this field, or whether your work is increasing. But I think any of us who run computers would have noticed the growing sophistication of the way in which fraudulent approaches are being made to people using electronic communications. There is a growing awareness in the financial sector that even some of their services are quite vulnerable—I think the banking system

is starting to look at additional protections for their online banking systems and the like. There is surprisingly little activity reported there if it is one of the major focuses of the ACC, or am I misunderstanding the environment? Perhaps state police forces or the AFP are doing this and you are doing the intelligence—I do not know.

**Mr Milroy**—Before Jeff comments, I indicate that in this environment in particular there are a number of agencies that would lead in certain areas. As you know, there is the Australian High Tech Crime Centre and the AFP, of course, have a significant role in terms of identity crime. We have a certain responsibility in this area in relation to the special intelligence operation on identity crime and card-skimming which allows us to use coercive powers to enhance intelligence and knowledge in this particular area. So we have been working in partnership as we are developing more knowledge to provide more advice to the board for their consideration. At the same time, we work in partnership with the various state and federal task forces which are dealing specifically with identity crime—the AHTCC, of course, have had more to do with the computer and phishing issues. That is the environment that we are—

**ACTING CHAIR**—Sorry, who has more to do with that?

**Mr Milroy**—The Australian High Tech Crime Centre. We of course are still in the process of collecting intelligence from those areas so that we can better advise the board on the total problem of ID crime, but we have a specific role to play in certain areas and a complementary role to play in other areas—for example, in the Identity Protection Register. In other areas it has been acknowledged we have taken the lead and use world's best practice. Jeff might expand a bit further on the overall question, if you wish.

**Mr Pope**—You will note Project Carlby is mentioned on page 48 of the report. In that project we seized 700 fraudulent credit cards. I actually managed that investigation at the time and it was quite a complex investigation to do. In a special intelligence operation the advice from certain legal sources is that you do not have the ability to use things such as telephone intercepts and listening devices and other such investigative assistance that you would otherwise draw upon. Therefore, as a special intelligence operation we concentrated mainly on collecting the intelligence and not so much on effecting arrests. For this particular job we brought in two investigators from the major fraud investigation division within Victoria Police to assist.

Since that job was reported, the intelligence that we gleaned from this particular investigation, or special intelligence operation, led to the detection of another 2,200 skimmed and fraudulent credit cards at Sydney Airport, which was a significant seizure and the largest seizure by Customs at the time, as I understand it—it was in about June of last year. I could go much further with respect to this particular group, but I would be reluctant to do so in a public hearing. Suffice to say that the special intelligence operation was confined by the inability to use some of those covert sources, if you like. It specifically concentrates on collecting the intelligence, understanding the environment, advising our partners as to the emerging trends and looking for law reform opportunities.

**Mr WOOD**—I know you mentioned solutions before, and I am not sure if it comes under your umbrella or not, but have you looked at making recommendations regarding biometrics et cetera?

**Mr Pope**—I have certainly been a part of a number of discussions at working parties and other sorts of meetings where biometrics has been discussed. The ACC had been represented on working groups such as the AUSTRAC proof of identity steering committee and other such groups where biometrics has certainly been discussed as an option.

**Mr WOOD**—I suppose I am asking: in your professional opinion, would biometrics help reduce the fraud—that is my own opinion, but I am seeking your opinion—whether it be by iris, voice or whatever else?

**Mr Pope**—Biometrics does have advantages, but there are weaknesses in the current proof of identity framework that challenge the successful implementation of biometrics. That is my view.

**Mr WOOD**—Are you saying that the technology is just not there at the moment?

**Mr Pope**—No. I am happy to go further if I can discuss it in camera.

**Mr Milroy**—I think we should point out that the ACC is not classified as an expert in this field and it is not part of a brief; we are there to collect a lot of intelligence on identity crime. As I mentioned, a number of agencies are recognised as having the lead in specific fields. The whole idea of the special intelligence operation is for us to bring the force of powers to complement the work that they are doing and for us to be able to leverage off the operational groups who have the ability to carry out investigations and use telephone intercepts and listening to devices. We move along with them, gather the knowledge and then present the findings, with certain recommendations, to the board. If the board then feels, based on the available information, that it is justified to set up another task force, which specialises in this area, to work on a specific crime syndicate then so be it. The partnership we have with a number of agencies across a raft of areas in ID crime is working quite well, but there are some areas in which we are not an authority and I think it would be inappropriate at times to form opinions.

**ACTING CHAIR**—I suppose it is implicit that some of this questioning goes back to intelligence and the threats assessment and where that sits in the hierarchy of threats to Australia in serious and organised crime. If it were low down, you would not expect to be engaged in a way other than you have described. Certainly, as a layperson and a person who is increasingly aware of their own vulnerability in the use of these things—maybe wrongly—I start to suspect that there is a degree of risk in the use of some of these things and that a lot of people out there are trying to make money out of abuse. I am just wondering where the hierarchy of threat and the criminal environment sits in your perspective. It is obviously not violent or what have you, but the costs to the community could be very large.

**Mr Milroy**—We acknowledge that identity crime is a facilitator for nearly all of the sorts of crimes that are carried out by serious organised crime groups, and one has to be conscious that they continually keep adjusting to technology and finding ways to defeat it. I think it is important that, when we operate with our partners in any of these areas, we have consultations over operational activities in confidence and that we are forever aware of changing technology, what criminals are using and what we, in partnership with others, will need to do to counter the effects that has on our work. As I indicated, there are some areas in which we are not an expert, but we can surely provide the committee with further information if you consider that appropriate.

**ACTING CHAIR**—We will obviously have an opportunity to discuss this in contexts other than the annual report. I would be interested to see the public version of your next *Picture of criminality* report, if there is a public version—I assume there will be.

**Mr Milroy**—So far there has not been. Certain statements have been made from the previous report. It is a foundation document that leads into the national criminal intelligence priorities, which are then determined by the board and communicated. Some parts of it are communicated in the public domain.

**Mr Brady**—I would just add, in relation to identity fraud at large, that a lot of those offences come up in the course of the ACC's other work, other arrangements and the work of partners more broadly. In fact, very few sophisticated crimes do not have an identity fraud element. But this is a special focus from an intelligence and complementary powers perspective trying to elevate the status of knowledge, rather than attacking the identity crime as it comes up in the course of other investigations. But virtually every job has that element.

**Mr RICHARDSON**—I know that some of my ex-state police colleagues are very hamstrung in this area by the long time that an investigation such as this takes and the complexities of it. Jeff, I encourage you to continue the good work that you have done towards prevention. But if at some stage you see a significant element of criminality within this field, I know that our state colleagues across the board are screaming out for that assistance. We would love to see some prosecutions rather than just prevention, which is also difficult. I guess that was more a statement than a question.

**Mr BYRNE**—Leading on from that, you said that you have laid 626 charges. How many convictions have arisen out of those charges?

**Mr Milroy**—We can provide the details specifically relating to 2003-04. Some of the prosecutions, of course, are against some fairly significant targets who normally fight fairly vigorously to defend their position, and sometimes they take 18 months to complete. But we have had a number of people who have pleaded guilty and a number who have received fairly significant sentences: 24 years-plus. We can provide that to you in relation to some of these cases.

**ACTING CHAIR**—It is one of the things that would assist in the report, although each year is obviously a snapshot of what happened in that year. Looking at our assessment and the public's assessment of the organisation as a whole, it would help to have the tracking of the progress of matters as they proceed through. For example, in this year you point out that 200 and some individuals have been the subject of charges and 600 charges have been brought and that there have been confiscation orders sought for so many millions of dollars. It would be useful, in providing some flesh to this, for each year's reporting to report on the 'carry through', as to how these things actually work out. Not every prosecution will be successful; we would not expect that. But it would still be useful to have a snapshot that also picks up the past to some extent, so you get a qualitative sense of how this all works out.

**Mr Milroy**—Yes. I notice in the report, in appendix E, there are some court results but, as you know, some of them go back nearly two years. Some successful prosecutions at the moment

even go back to the days of the NCA, and people have been in custody for three years. I think we could show progressively the results.

**Mr BYRNE**—In relation to the people who are trafficking for sexual exploitation, can I get a quick snapshot as to your agency's involvement in that particular operation?

**Mr Milroy**—This is people trafficking?

**Mr BYRNE**—For sexual exploitation.

**Mr Milroy**—Again, this is an area where the ACC initially carried out an intelligence probe 18 months or so ago, when we thought it was an issue emerging. Then the board subsequently approved—following our consultation with the Federal Police and DIMIA, who are lead agencies in these areas—that the coercive powers would be very beneficial both to the Commonwealth and the state agencies to, again, improve our knowledge but at the same time utilise the powers to examine some of these ladies who have been brought to this country for sexual servitude.

This matter will come before the board at the next board meeting in May for further consideration because the determination period is coming up for review. We have been carrying out a number of examinations across the country in consultation with DIMIA, the AFP and also state jurisdictions. We have seen a greater understanding of the benefits that the coercive powers can bring to state and Commonwealth investigations. It has taken us quite a while to educate people about the benefits of putting some of these persons before the hearings to try and identify who has been responsible, how they actually came to be in the country, how they got their visas, where this money is going, where the control is and who is controlling them. Those results will be presented to the board in May.

**Mr BYRNE**—In your output measure in that area for the period 2003-04 you are talking about two examinations held under section 28 and one under section 29. Would you be expecting to see in the next annual report that far more of these examinations have been conducted?

**Mr Milroy**—That is correct. As the committee would be aware, of course, the PJC did hold a public hearing in relation to this. I think the committee said it would be interested in seeing the results of our work over the next 12 months. That period is nearly coming to completion, and we will hopefully be in a position to provide you with some further information.

**Mr BYRNE**—With respect to that, where is most of this people-trafficking originating?

**Mr Milroy**—We are seeing some changing trends. Most of it is from South-East Asia, but we have noticed—and, again, this is something that we have to present to the board, not in a public hearing—some changes from one region to another as a result of corrective action that you might recall was put in place by the Commonwealth government and also the countries concerned. We then see a shift, depending on the circumstances, of people coming from another region. We are also monitoring the effect that this is having in Europe and in the UK because people-trafficking is a global problem. We are looking at what trends are occurring globally and whether that has an effect on the Australian market. So we are noticing some changes. As I said, we have only been doing some of these more in-depth hearings for the last three or four months

and we are starting to see some trends that hopefully will provide the board with sufficient information to consider the future of this determination.

**Mr BYRNE**—For my information, is the endpoint of this with, say, the South-East Asian crime gangs et cetera that operate in Australia? You are indicating that there has been a change. Does that mean that there are other elements operating here within the organised crime group that are organising this?

**Mr Milroy**—What I mean is that where, for example, the intelligence indicates that people from one region have actually been able to facilitate this process, these findings have been communicated—bearing in mind that the Australian Federal Police are the lead agency with DIMIA—and as a result these agencies have been able, through discussions with foreign agencies and governments, to stop certain activities in those countries and also in relation to the movement of people to Australia. What I am saying is that if there is a market, then of course somebody else from another area steps into the market and tries to fill in the vacancies, if you might want to call them that, that are available. Again, the results of this ongoing work by the three agencies will be considered by the board.

**Mr BYRNE**—Is people-trafficking a growing issue?

**Mr Milroy**—I am not in a position to comment on that.

**Mr BYRNE**—At some stage in an in camera discussion later on, not tonight, would we ever get further information about these matters?

**Mr Milroy**—Yes. I believe that the committee did indicate, when it held a public hearing, that it wished to call the relevant parties back for an update, in particular as to the outcomes of the coercive powers. We will be in a position to do that.

**Mr KERR**—Chair, we have looked at output 1.1 and 1.2.

**Mr RICHARDSON**—I have one question in relation to coercive powers and the auditing of warrants to be executed or warrants that were utilised through the reporting period. Is there an audit process for those warrants used to enter premises et cetera?

**Mr Brady**—Are you referring to search warrants?

**Mr RICHARDSON**—Yes.

**Mr Brady**—Each of the warranting processes—the search warrants, telephone intercepts and controlled operations certificates—has its own separate regime. I think you spoke to the Ombudsman last week, so you would be well aware that there is a special regime for controlled ops. Telephone intercepts, again, are monitored by the Ombudsman's office. They look at specific documentation and the follow-up reports, as they are required to under the act. With the search warrants, the legislation does not have that same sort of process. Of course, the major test for a search warrant is always going to be when you are facing the admissibility in court. Increasingly, we see that tested by people for a whole raft of reasons, not the least of which is

that frequently there is very compromising material and they need to attack that evidence—as they have the right to do.

We have a raft of internal integrity processes. To my knowledge, we do not specifically focus on search warrants per se unless we have a reason to look at those. But the major test for the proper exercise of search warrants is always going to be in the court process, the judicial processes, unless there is some particular issue that has arisen, such as someone has claimed legal professional privilege or some other form of privilege and it is tested before they get to committal and trial. We have had a few of those. We have processes in place which are accepted by the Law Council as to how we conduct searches in lawyers' offices and what not. That is normal police process. Each of our seconded forces is still subject to their commissioner's own instructions for their jurisdictions, and we comply with that. There is a labyrinth of different issues, but we do not specifically audit search warrants unless there is a particular reason to do so, such as some suspicion about an officer's conduct or whatever.

**Mr RICHARDSON**—And, like you said, you do not tend to find out until such time as the court process. However, it may be advantageous to do one or two a year.

**Mr Brady**—The fact is that we have multidisciplinary teams. Pushing forward lawyers for change—not many people do—part of our team lawyers' role is to proactively reduce risk so if there is an issue that needs to be addressed it is addressed before we seek the search warrant. If there is anything peculiar in the documentation we always seek to stop using it until we have fixed that. Mistakes do occur in every warranting process from time to time—misdemeanors, mistakes and what have you—and I think that the multidisciplinary team at large is a good risk minimisation strategy because the chance of particular people acting alone is reduced. It is not eliminated, but it is reduced.

**Mr BYRNE**—There is a time lag sometimes of, say, three years or so, which is what Mr Wood, as a former serving police officer, was saying. If there is a problem in that warrant, you could have three years of warrants being issued that might not be technically correct.

**Mr Brady**—You do find that committals come up much faster in, say, New South Wales with the changes to the way the committal regime now operates. In fact, the delay between committal and trials reduced dramatically too.

**Mr BYRNE**—What is the average time frame, then?

**Mr Brady**—I know that the average time frame between committal and trial has been reduced in the District Court to about three months, which is quite short—some people are complaining that they have not got time to prepare their defence. I do not know whether we have actually looked at it from a risk management point of view to see whether or not we need to focus specific processes in this area of search warrants. I do not think our experience has shown that we have had significant numbers of problems in that area.

**Mr WOOD**—Would there be concerns, though, if you allowed people outside an investigation to actually view a search warrant? To me, that may jeopardise the investigation.

**Mr Brady**—There have been no discussions to date to do this but, technically, the Ombudsman could conduct an own motion investigation into anything we do. In fact, you would be aware that he has done one for our use of state controlled ops. There is certainly nothing to stop us from applying a risk management process and deciding that we will do some auditing of search warranting processes. From time to time, I get lawyers mentioning to me points of discussion around search warrants. It is a hotly contested area and I think most of them do come out in the judicial process.

**Mr Milroy**—We do acknowledge that it is an area of risk—not only the issue of the warrant but also the execution of it and what goes on at the time of the search. We have actually carried out a risk assessment: we brought in an expert to look at all the risks across the organisation and come up with risk checklists. The issue of warrants and the execution of warrants of course fall into that risk area, and it is going to be audited. The fact that we have multiskilled teams with lawyers as part of them operating as secure cells is one thing, and we should not be complacent, so we will take on notice the committee's comments about some sort of auditing process, even though we do have a random process in place.

**CHAIR**—We will move on to output 1.3. Are there any questions?

**Mr RICHARDSON**—Mr Pope, on human resources: you mentioned that the commission employed 518 people at 30 June 2004. This was an increase over the figure given at 30 June 2003. The main area of increase was in staff at APS level 5 to executive level 2. Why the increase in staff and particularly why in the range of middle management?

**Mr Milroy**—Mr Phelan will answer that shortly, but I might indicate that there was a total of 506 staff or thereabouts when the organisation was established at the time of the merger. One of the issues that the ACC considered is the skill base that is required for us to perform our functions as set out in the act. We went through a process of looking at what skills and what recruitment program we required. We looked at an interim structure and then we moved to a new structure in December and have done some finetuning recently. So we were conscious of the requirement to get the mix of staff right and that led to the variations in staff numbers and skill base. Regarding the APS staff, you have to realise that that figure was the number of positions we identified as a requirement to have some continuity in management and to own our own people, although there is a component which is seconded. We went about developing the structure and identifying the levels that we required. In some areas, of course, such as with the very high risk areas like the covert group and with some of the higher level people, it is hard to get the right skill base on board. Mr Phelan can probably cover off in relation to the numbers between APS5 and EL2 that you referred to.

**Mr Phelan**—I think you have said it all. It is mainly the need for professional staff in legal, investigative and analytical areas. They are not middle managers per se; they are in structures which require us to offer a competitive wage and, in the Public Service environment, that tends to be at the APS5 through to EL2 levels, particularly for lawyers, for financial analysts, for analysts generally et cetera. So there has been no growth in middle management—in fact, quite the contrary: it has been a growth in people with the requisite skills to deliver our outputs.

**Mr KERR**—With regard to output 1.3, which involves your financial seizures, in our last comment on the ACC annual report we raised the point that it was simply an aggregate figure



rather than a breakdown of the numbers of matters to which those figures relate. That appears, unfortunately, to be reflected in this report also. That may simply be because that particular comment was not noted. Is there any reason why we could not have the disaggregation of those figures?

**Mr Milroy**—Are we talking about the figures to do with the tax assessments or the proceeds of crime?

**Mr KERR**—The proceeds of crime and tax assessments.

**Mr Milroy**—So you are referring to where it says, for example, ‘seized 3,552 firearms through 55 seizures’, and you are asking about the \$19 million and what it equates to.

**Mr KERR**—In the area I am looking at you have reported that assets of \$1,581,200 have been restrained. That does not refer back to the number of matters that relates to. It could be one large matter or it could be several minor matters. It would just be useful to know.

**Mr Milroy**—Yes, I think that is a very valid point.

**Mr KERR**—The other thing is, I assume that when you talk about tax assessments those are ones which you can attribute directly to your participation. The intelligence work that you supply into the tax system may be responsible for larger collections, simply because the tax office becomes more refined and more effective in its operation. I do not know. Again, it just seems strikingly low as a figure. I am not meaning that that suggests inefficiency on your part, but if bad guys are being disrupted all over the place you would expect there to be relatively higher tax assessments being issued as their criminality becomes exposed.

**Mr Milroy**—That mainly relates to the work that we do under the Midas determination.

**Mr KERR**—That is a Midas reference directly?

**Mr Milroy**—That is right, yes.

**Mr KERR**—All I am trying to say is that you may be too modest. I am just wondering whether there is any way of reflecting, if that be the case, the fact that tax revenues actually may benefit to a much larger degree than is reflected in those, I would say, modest amounts.

**Mr Milroy**—Yes. I might ask Mr Newman to comment, because we have been asking discussions with the tax department on that very subject.

**Mr Newman**—Mr Kerr, you are right in the sense that there are obviously greater assets seized et cetera from direct results of our dissemination of intelligence. Mr Milroy mentioned in his opening address that we are looking at an effectiveness and efficiency framework for the organisation. We are in the process of capturing the value of the intelligence not just in terms of proceeds of crime but maybe in terms of seizures and other results where it is not as a direct result of what we would call our direct operational activity but as a result of the dissemination of intelligence or our partnerships. So we would expect maybe not to be accounting for and counting all of that in our report but to be acknowledging that it has led to those seizures.

**Mr Brady**—I think it was in the NCA days that, for an operation called TUBU, the tax office had done some estimates of the deterrent value of that job. I am just working off memory now, but I think there was a figure of some \$90 million of additional compliance in future years. Those sorts of jobs do not come up that frequently. It also depends on where you are in the cycle, because a lot of those jobs take many years. But we are doing some work at the moment which is likely to have those sorts of broader impacts.

**Mr KERR**—Yes. I am not trying to suggest you can quantify these precisely, but if you were able to have a similar sort of discussion with the tax office and to try and, in a sense, identify in your report the value added that comes about—not merely as direct and attributable seizures but reasonable estimates of the value adding that is contributed to by your intelligence work or perhaps even your direct operational work—I think it would be helpful. The actual numbers—albeit that I would like to have that amount of money given to me; it would make my life very comfortable—nonetheless sound quite modest when you consider the sorts of resources that you would expect to be available by way of the contribution that you add.

**Mr Brady**—Certainly with TUBU. The matter that we are currently looking at is scheme promoters, and it is with schemes that you tend to get a huge deterrent effect in the next cycle because the scheme stops. Whereas if you simply take out the unpaid taxes for one target there is not necessarily that same consequential impact.

**Mr WOOD**—With regard to corporate and financial, 1.12, I note with interest the corruption charges of police officers. Without getting into any specifics, the one thing I do have a bit of interest in is that obviously you are getting members from various state and territory police services, and they would come under the recommendation of a superior officer. Do you actually go to the extent of viewing a member's personnel file—which I would strongly recommend—not just in case charges have been laid, whether internally or through a court process, and have been found to be nonsubstantive but because, importantly, there may be concerns raised within the member's personnel file which would make them unsuitable?

**Mr Milroy**—I can indicate that the vetting requirements for seconded officers to come to work for the ACC are a lot stricter and at a much higher level than the former agencies'. The board members actually have to sign off on those individual officers' integrity and suitability to come to the ACC. In other words, there is a recruitment process and a recruitment panel that our department and the relevant agency manage professionally. Then the selection of those officers goes through to the police department concerned. The commissioner ensures that those officers are screened within the department. The commissioner is then requested by us to sign in writing that that officer is suitable and cleared to come to the ACC.

**Mr WOOD**—I know how boards work. They do not actually have access to members' personnel files unless they go through an appeal process. This is what I am saying. The superior officers sign off a report. I would like to think that they have actually reviewed the member's personnel file so that they would be aware of someone who may have been linked to some sort of drug inquiry rather than them not being aware of it.

**Mr Milroy**—Board members have indicated to me at board meetings that the integrity process within their departments will be monitored by them. Those processes vary, of course—as you know, each police department has a different process. Those integrity commissions et cetera will

be utilised. The commissioners are fully aware of the process that they are required to comply with within their jurisdiction before they sign off on an officer who has been through a very vigorous recruitment process, which we participate very thoroughly in.

**Mr Phelan**—The evidence we have is that it is very thorough and does include access to those files.

**Mr WOOD**—That is all I wanted to hear.

**Mr Phelan**—We then overlay that process with our own vetting process to bring people up to Commonwealth ‘highly protected’ levels. That involves quite intrusive financial checking, reference checking and, on occasion, face-to-face interviews with not only ourselves but also some of the other spookier agencies around the place.

**Mr KERR**—Mixed up in all this, of course, is the interjurisdictional nature of the ACC. We had some discussion the other day with the Ombudsman which drew to our attention issues with controlled operations—the fact that the vast majority are actually conducted under state jurisdictions rather than by the ACC. That raises issues of complaints. It raises issues of the equivalent of cost shifting—that is, choice of jurisdiction—when the Commonwealth parliament erects certain kinds of regulatory frameworks. I understand there are ongoing discussions about some of those particular issues with the Ombudsman. In the larger context, has there been any work undertaken with you and your partner agencies about some kind of joint oversight cooperation—most of the states have equivalents of the Ombudsman—so that there are no gaps? If there are gaps, such cooperation would, firstly, identify where they are and perhaps encourage those states to fill those gaps; and, secondly, with respect to complaints and disciplinary measures, make sure there is a seamlessness so that you do not have this awkwardness, I suppose, that must be confronting you constantly in terms of personnel management.

**Mr Milroy**—First of all, I will ask Michael Outram to just explain from a practical point of view how he and operations have to deal with this, and then Peter will provide you with information about the current processes we have in place with the Ombudsman’s office and the state bodies in order to adequately manage this.

**Mr Outram**—Firstly, all the operational activity that we engage in has to be approved through our own internal governance processes. First of all we have the determination, which of course is approved at the board level, and then internally we have a governance operations committee, of which I am the chair. The CEO sits on that, as does the director of intelligence and others. We get a fortnightly update in relation to each investigation operation, whether it be an intelligence operation or an investigation, and any activities such as controlled operations, covert activities et cetera are reported. We also have a fairly rigorous process of looking at our human resource allocations to make sure that they stack up against priorities. As Peter mentioned earlier on, each multidisciplinary team has its own lawyer and there is, as you rightly say, a plethora of different state and Commonwealth legislation that sometimes is complementary and sometimes is not. The approach we take with our lawyers is that we use the most appropriate legislation. If it is primarily a state offence that we are looking at with a partner agency and there is legislation available, we use that. If it is a Commonwealth offence, we use the Commonwealth legislation.

In relation to partner agencies, if we are in a task force arrangement of course it could be more difficult, but even the national task forces are brought in under the governance umbrella, if you like, of the ACC, so decisions to undertake controlled operations will not be taken outside our governance processes. Certainly, if they were, the approval processes, the lawyers' decision making and the resources would not be deployed from the ACC. So we have a fairly good coverage in all those areas. Also, we collate the information on all controlled operations centrally, whether they be state or Commonwealth based. Peter will correct me if I am wrong, but when the Commonwealth Ombudsman comes in we declare all controlled operations activity in that audit, in order to show transparency. If there are some issues where perhaps we need to pay attention, we can obviously get that feedback from the Ombudsman and do so.

**Mr Brady**—The only other thing I would add is that members of the committee are aware that one of the outcomes from the 2002 leaders summit was that there was to be a working group to look at the harmonisation of key investigative powers across jurisdictions. That touched on four areas: surveillance devices legislation—and the Commonwealth has since passed an act; controlled operations; assumed identities; and the fourth one I think was witness anonymity. Model legislation was designed. Some of the states—Queensland, for example—argued in the case of surveillance devices that they had a slightly higher watermark with their public interest monitor, but the core legislative model is the one that is going forward. Victoria has passed an act, but interestingly it has not been proclaimed to commence yet, because I think the machinery is not in place for it. So, for surveillance devices and controlled ops, there will be a fairly consistent approach, if not in terms of the legislation in each state, at least in recognition of approval mechanisms from other states into another jurisdiction. One issue I know—and I do not know whether the Ombudsman has raised this—is the question of whether, in the case of the ACC, the Commonwealth Ombudsman will do all of the ombudsman inspection for our agency or we will have to have umpteen different ombudsmen's audits.

**Mr KERR**—I suppose that was the point I was getting at: whether you were working on trying to develop some arrangement with partner agencies where there would be at least either an agreement or a legal framework that would enable there to be efficiencies—it could be the Commonwealth doing it or it could be a shared arrangement, but at least making sure that the system is fairly seamless.

**Mr Brady**—Lionel will correct me if I am wrong, but our agency's position is that we will comply with whatever governments collectively want us to do. My understanding is that the Commonwealth A-G's Department is looking at negotiations with the other states so that the Commonwealth Ombudsman will pick up the role for the ACC—and there will have to be some cross-vesting powers—for all jurisdictions. It is not something that affects the AFP at the moment—it may well pick up powers in other states as well—but it is primarily an issue for us.

The other thing to do with controlled operations is that they are all approved by only two people in the organisation for our internal approvals. For external approvals we gather all of the documents together and they get inspected as well. That is a subject that the Ombudsman's meeting with you last week touched on as well. There have been a couple of approvals under what I would call common law arrangements. These are for jurisdictions that do not have any scheme. What we have sought to do there is deal with the Ridgeway test by applying the process from the Commonwealth internally on an informal basis, so that our staff, using our lawyers, will have to put it on an application document. Some members may be aware of the discussion

that occurred in the Senate when the Commonwealth act was approved. We are seeking to make sure that any person who conducts themselves in undertaking certain types of activities best places themselves to be able to get an immunity from the Commonwealth DPP after the event. I am talking particularly about civilian operatives. It would not apply to the Commonwealth because the Commonwealth act does not cover that, but for some states there is no scheme at all. For example, with Victoria there is only a provision in relation to drug trafficking, it is put as an officer of the rank of senior sergeant or above and Victorian police can approve certain conduct. We have issued only about two or three of those common law directions to staff. Again, we have a register; I have mentioned it to the Ombudsman. In due course when the next inspection period comes around they will be having a look at those too.

**Mr RICHARDSON**—My question comes under finance. Mr Milroy, I do not know who the finance man is but finance is always a question that comes into it.

**Mr Milroy**—It depends on what the question is.

**Mr RICHARDSON**—The commission's budget appropriation for 2003-04 was \$65.4 million. In the previous reporting period it was \$65.1 million. The commission had a deficit of \$3.3 million. In the previous year there was a small surplus, which included an operating loss of \$1.4 million. The report explains that about half the deficit was attributable to a write-down of assets. Why did the operating loss occur? Where was the additional expenditure incurred?

**Mr Phelan**—We were intending to spend, as we explained at page 87, moneys that had been appropriated in previous years and had built up as a reserve. The original projection was a deficit of over \$4 million. That is an accounting consequence of spending in one year moneys appropriated in a previous one. What we were spending in that year—that is, the year in which we incurred the deficit—was on the introduction of the Sagan covert intelligence unit capability for which funds had been appropriated to the NCA in previous years. But what we managed to do during that year was in fact mainstream that expenditure by producing economies in various other areas to do with travel and so on. So we brought the projected operating deficit down from \$4.5 million to \$1.4 million but we used the opportunity to clear the decks with a lot of assets that were carrying values that were inflated for historical reasons. For example, we had moved on in terms of the size of our leasehold premises in Melbourne so we needed to reflect the fact that we had several hundred metres less space. That in turn produced a write-off of certain fit-out valuations.

There were other assets that had valuations as to lives that were untenable—computer systems, for example. One of the big ones was in terms of telecommunications interception where we had decided that the software was becoming more obsolete as we were planning to introduce new software and a new system—which we have since done in this financial year—so we took the opportunity to write that down. The consequences of the asset write-downs were to inflate the loss in that particular year and to reduce the potential expenditure in respect of those assets in subsequent years. That is what I mean by positioning ourselves for more asset acquisition and infrastructure enhancement in these particular years. That is in a nutshell where the pressure points were at the time and why the expenditure occurred as it did.

**Mr Milroy**—It was about getting the house in order.

**Mr RICHARDSON**—You did a good job.

**CHAIR**—There being no further questions, I thank you, gentlemen, for coming in and being of assistance to the committee. We look forward to seeing some of you, if not all of you, tomorrow morning.

**Committee adjourned at 7.40 p.m.**