COMMONWEALTH OF AUSTRALIA

Official Committee Hansard

JOINT SELECT COMMITTEE ON THE INTELLIGENCE SERVICES

Reference: Review of intelligence services bills

WEDNESDAY, 1 AUGUST 2001

CANBERRA

BY AUTHORITY OF THE PARLIAMENT

INTERNET

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

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

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

JOINT COMMITTEE ON THE INTELLIGENCE SERVICES

Wednesday, 1 August 2001

Members: Mr Jull *(Chair)*, Mr Andrews, Mr Brereton *(Deputy Chair)*, Mr Forrest, Mr Hawker, Mr McArthur, Mr McLeay, Mr Melham and Mr O'Keefe and Senators Calvert, Coonan, Faulkner, Greig, Sandy Macdonald and Ray

Senators and members in attendance: Mr Hawker, Mr Jull, Mr McArthur, Mr McLeay and Mr Melham and Senators Ray and Greig

Terms of reference for the inquiry:

To inquire into, and report upon:

(a) the Intelligence Services Bill 2001 and the Intelligence Services (Consequential Provisions) Bill 2001; and

(b) the provision in the Cybercrime Bill 2001 relating to the Australian Secret Intelligence Service (ASIS) and the Defence Signals Directorate (DSD)—Liability for Certain Acts.

WITNESSES

Committee met at 9.05 a.m.

BLICK, Mr William James, Inspector-General of Intelligence and Security, Office of the Inspector-General of Intelligence and Security

BONIGHTON, Mr Ronald Bruce, Director, Defence Signals Directorate

CARMODY, Mr Shane Patrick, Deputy Secretary, Intelligence and Security, Department of Defence

CHAIR—I declare open this hearing of the Joint Select Committee on the Intelligence Services and welcome witnesses and members of the public. Today the committee will take evidence from the Defence Signals Directorate, the Australian Security Intelligence Organisation and the Australian Secret Intelligence Service.

Although the committee does not require witnesses to give evidence under oath, I advise witnesses that the hearings are legal proceedings of the parliament and warrant the same respect as proceedings of the House or the Senate. The giving of false or misleading evidence is a serious matter and may be regarded as contempt of parliament. I invite you to make some introductory remarks before we proceed to questions.

Mr Bonighton—While the Intelligence Services Bill 2001 is primarily a piece of legislation for ASIS, there are a number of sections which also relate to the operations of the Defence Signals Directorate. I appreciate the opportunity to appear before the committee to address those issues. Like ASIS, DSD has been operating under a government directive. The inclusion of DSD under this legislation will allow for the directorate's functions to be articulated in legislation for the first time, and for that reason alone I welcome this bill.

The bill also outlines the accountability mechanisms for DSD and reinforces the role of the Inspector-General of Intelligence and Security in his oversight of DSD and other intelligence and security agencies. Again, I welcome the bill for the clarity and visibility that will be provided for under these provisions. Finally, the Intelligence Services Bill will provide for limited legal liability for the directorate in the proper performance of those functions. That will allow DSD to continue to perform those proper functions in accordance with the requirements set out by government.

We believe our situation differs from that of ASIS and ASIO in that DSD is fundamentally one of the six outputs—that is, part of the intelligence output—of the Defence organisation. We are a core element of that Defence intelligence group and we remain closely integrated with specialist units of the Australian Defence Force. Indeed, many DSD staff are military personnel who rotate from DSD to specialist ADF units and maintain the strong linkages and interconnections between DSD and its major customers in the Australian Defence Force.

Under this bill, oversight for DSD will continue to be provided through our direct involvement in the Defence financial and administrative process, and through my line accountability to my deputy secretary, the secretary for Defence and, ultimately, parliament through the minister. As is the case for each of the outputs of the Defence organisation, the opportunity for parliament to perform oversight of that output exists through the mandate of the

Joint Standing Committee on Foreign Affairs, Defence and Trade and the Senate standing committee as well.

The legislation provides for ministers to make rules to protect the privacy of Australians. DSD already operate under such a regime, which has been approved by government. Our adherence to those rules is audited by the Inspector-General for Intelligence and Security on a regular and routine basis. DSD's role is to collect foreign intelligence. We take very seriously our obligation to respect the rights of Australians to privacy.

I will conclude by saying that we are very proud of our history of supporting the ADF and the government and in securing their communications. This legislation will allow DSD to maintain that capability in a rapidly changing technological environment and to ensure that DSD continues to fulfil its role in supporting Australia's national security.

CHAIR—Thank you. During yesterday's hearings the issue of cryptography and, indeed, your role in providing services to all levels of government arose. The functions that you have are set out in clause 7(d), but I was wondering if you would be prepared to enlighten us a little more on your exact responsibilities and what you do in that regard in the provision of services to government.

Mr Bonighton—Certainly. Cryptography covers a fairly wide field. It covers both the construction of codes and security devices and their deconstruction or decryption. The role we play for government is one of providing all key material for government authorities, so it is our responsibility to ensure that the high-grade ciphers used by government are secure. We also provide advisory services to government authorities on their IT security. We also evaluate specific security products and publish an evaluated products list that provides guidance for agencies on the sorts of equipment and security devices that they should use in order to protect their communications.

CHAIR—So, really, the work that you do does not go beyond government?

Mr Bonighton—It does not go beyond government. It can go to the states in very limited instances. For instance, the Olympics was one area where it was not so much a cryptography problem as a distribution of intelligence. We do not distribute intelligence to state authorities. What we were looking for was a mechanism by which we could get, say, indications of terrorist activity very quickly to the New South Wales state police, who were responsibility for Olympic security. We had plenty of warning on how we might be able to do that. In fact, ASIO set up mechanisms that allowed us to make sure that information would flow. But we are a foreign intelligence collector; that is our focus.

CHAIR—For the record, you would not be involved, for example, in providing specific advice or setting up systems for a state police force?

Mr Bonighton—Not at present. We could provide advice if they came to the AFP and said, 'We need advice on this.' The AFP might then come to us and say, 'We need advice.'

CHAIR—But it has not happened to date?

Mr Bonighton—It probably has in a very small number of instances. In some cases, we might not know that the AFP are inquiring on behalf of a state police force. But we would see it as part of our advisory role. I do not think there is much to be gained by allowing our police forces to operate with insecure communications if there is a product on our evaluated products list, for instance, that they could be encouraged to use.

Senator ROBERT RAY—I have a number of questions, but one of the purposes of these public hearings is to gain an understanding of your organisation. Because there is not much exposure to organisations like yours, there is not always a lot of understanding of safeguards. I suppose the biggest concern for the public—not that it is a big concern, but it is a concern—is the targeting of Australia citizens. Would you like to take us through the processes. You say that you target overseas material. Could you take us through the process of what happens when, coincidentally, an Australian is involved in that process?

Mr Bonighton—Should we come across the communications of Australians in the course of our normal activities, we would immediately stop any intercept on recognition that that was an Australian communication. Should we be in a situation where an Australian is named in the course of other intelligence material we come across—it is discussed, say, by other people—we would expunge that name from any reporting we might do and from any database that we had.

Senator ROBERT RAY—Can you assure us that that all files are open to the Inspector-General of Intelligence and Security to check that you have complied with this?

Mr Bonighton—Absolutely, and that is something that we push very hard in all our induction courses, in our training courses, to make sure that there is an ethos in the place that allows the Inspector-General that sort of access. I am not sure whether he was asked that question yesterday, but I hope he would agree that he has unfettered access.

Mr LEO McLEAY—I will take you back to the first question Senator Ray asked you: what would happen if one of your corresponding organisations targeted an Australian citizen?

Mr Bonighton—Before we enter into any exchange arrangements with other countries, we get undertakings from them that they will protect the privacy of Australian citizens in exactly the same way we do. In other words, there can be no question of our saying, 'We can't target this particular Australian but we'll ask someone else to do it.' We would not do that; it would strike at the very heart of the credence within our organisation of adhering to the sort of role we have.

Mr LEO McLEAY—Is that contained in the directives you have or is that just a philosophy that you have?

Mr Bonighton—It is partly a philosophy but the real guts of it is in the rules that are administered by the Inspector-General and that have been approved by cabinet; and they are quite detailed. One of the advantages of this bill is that I think we could tidy up some of those. Certainly, we will need to change the wording of them, and I think that would be a good time to review them.

Senator ROBERT RAY—Taking the interception a little further—you are tasked for specific purposes and targets—when information of a criminal nature comes to you as an incidental, are you entitled to pass it on to other relevant Australian agencies and, if so, under what conditions?

Mr Bonighton—Indeed. I guess the philosophical point is that I would not want to be in a position where I or my staff come across evidence of serious crime and we just sit on it. We would be compelled, I believe, to pass that to the relevant authority. We would need to make sure—and it is laid out in our rules—that if there is an indictable offence, a serious crime, that is what we should be doing. Each of those would then be examined by the Inspector-General. If there were any doubt on that issue, I would be at his office faster than a speeding bullet.

Senator ROBERT RAY—We have this dilemma that was raised yesterday that I do not think anyone challenges those procedures. But what you are in fact doing is alerting another law enforcement office to a possible criminal activity. They may then take it all the way through to prosecution. The person they prosecute, however, does not have access to your material. It may transpire that the material you have would go some way to clearing that particular individual but they have no knowledge that you have it, no access to it, et cetera, and that is put to us as a possible miscarriage of justice. What is your response to that scenario?

Mr Bonighton—I am not sufficiently versed in how the Australian criminal system works to really go through a case by case scenario. My role in life would be to make sure that, should that information be provided to the defence, it be done in ways which protect the source of that information. If that were not possible, I would be strongly taking the line that that prosecution might not go forward.

Senator ROBERT RAY—I am just wondering how you would know all that, though—how you would be able to follow that through. To use an example: you alert the Australian Federal Police to potential drug offences; they then take it from there, gather their own evidence and prosecute. How are you going to follow those intricate details to know whether some of the material you obtained in fact mitigates the AFP case against the accused? How are you going to know that?

Mr Bonighton—I can put it around the other way. Where the AFP might come to us and seek support in a particular case—say, an illegal immigration racket, a drug ring or something like that where there is an international or transnational aspect—we would get an understanding from them that any evidence we gave them would be not for evidentiary purposes, that it would be used for leads, follow-up and that sort of thing.

Senator ROBERT RAY—That is understood.

Mr Bonighton—They would then have to construct a case without our evidence.

Senator ROBERT RAY—I am sorry to interrupt you. It is absolutely understood that the material you give them cannot be used in an evidentiary way by the AFP or the DPP. The problem for the person defending the accused is that you may have material, in fact, that contradicts what the AFP go on to divulge but, because of the proper secrecy surrounding your organisation, they cannot ever have access to it, so there could be a miscarriage of justice. It is

true that we have the intermediary step of the Inspector-General who may realise this and be able to assist, but it is still a theoretical problem.

Mr Bonighton—I agree that it is a theoretical problem. It is a very small problem. Our involvement in these sorts of cases is quite small. That is not to say that a miscarriage of justice is not something we need to worry about. We certainly liaise closely if we are in a case like this with the AFP, but I agree that we would not have the follow through on a particular case to be able to make certain how that material was actually used, apart from the fact that it was protected.

Mr LEO McLEAY—If you were in a position where material that you initially provided started the AFP or someone else off on a matter, would you have a problem with the defence counsel or the defence team wanting to have access to a sanitised version of your material?

Mr Bonighton—I would be distressed if we got to that stage, because I believe it should be up to the AFP to construct a case which can stand up in court, independent of the sort of information we had. But if it came to the final push, we would then be looking at ways in which that could get to—

Senator ROBERT RAY—You are still missing the point, I am afraid. The AFP do build up their independent case. The history of our judicial system is littered with cases where the prosecution did not necessarily forward every piece of available information to the defence team. Here they have the classic excuse not to. It is properly protected DSD material and we do not want it around there, but it may have things in it that are contradictory to the case that the AFP has built up. Do you see the problem?

Mr Bonighton—I certainly see the problem. All I can say is that it is a very small problem.

Mr LEO McLEAY—I suppose, even if there were one, it is pretty important to the person whose case it is.

Mr Bonighton—I agree, and perhaps that is something we need to think about when the rules are recast, assuming this legislation comes into being.

Senator ROBERT RAY—The alternative is to allow the defence counsel in every case—which we do not like very much, I have to tell you in advance—to apply to the IG to see whether there was any DSD or ASIS involvement, and that could evolve into a delaying tactic or anything else. So you would probably be looking for another way to pinpoint such a case—giving the IG the power to try to pinpoint the case or something. In other words, we would like to see this solved but not create a massive bureaucracy to solve it.

Mr LEO McLEAY—Or if there were an outcome whereby you have a protocol with the AFP. You say that there are very few of these matters anyway. If you had a protocol with the AFP that said: if they get initial information from you to mount a case, there has to be a footnote on that saying that there was initial assistance given by DSD.

Mr Bonighton—I am willing to go along with any regime which provides protection for my material.

Mr LEO McLEAY—Clause 7 of the bill provides an outline of the functions of DSD. Could you tell the committee whether they are all the functions that you are doing now? Is there anything left out or added?

Mr Bonighton—There is certainly nothing left out in comparison with our directive. Clause 7(a), in fact, provides what I would call a fairly exact and technical description of what signals intelligence is, which was not in the original directive. I think we have already touched on the matter of our ability to advise state authorities. That has been added in to this on our information security side of the business. So that is additional to what is in the current directive and really tries to overcome some of the problems associated with events like the Olympics.

Mr LEO McLEAY—The Olympics do not happen all that often in Australia.

Mr Bonighton—Indeed, they do not. CHOGM is another one, I guess.

Mr LEO McLEAY—So if there is not going to be another Olympics here for a while, why is there the necessity for that? One of the arguments that was put to the committee yesterday was that for DSD to provide a substantial service to decrypt as well as encrypt would be a problem for civil libertarians.

Mr Bonighton—I would agree that it would be unfortunate to have a whole lot of state police authorities setting up their own decryption capability. I think we can foresee a time when we might, as the decrypter of last resort, if you like, provide some assistance to state police forces, if there were serious offences. The fact is that a country like Australia would not be able to afford to set up the sort of capability that DSD possesses. Without going into any specific details, that is a simple fact. On the other hand, I am not at all interested in having a whole lot of decryption agencies going about without the sort of national security regime and discipline that we have built up over 50 years. I do not want to see unique techniques get out into the public domain.

Mr LEO McLEAY—Thank you.

Senator ROBERT RAY—I have read the submission and I have heard what you have said today, and I hope you do not mind me describing it as weasel words on parliamentary accountability. I am trying to follow the reasoning why you do not want DSD under the purview of a sort of ASIS-ASIO committee. I have read it all and I have had a lot of experience in dealing with these sorts of mumbo-jumbo excuses—and that is all it is. But let us get down to brass tacks: when was DSD last properly examined in detail by a Senate estimates committee?

Mr Bonighton—Very rarely.

Senator ROBERT RAY—And by the joint committee?

Mr Bonighton—Very rarely.

Senator ROBERT RAY—By the Senate Foreign Affairs, Defence and Trade References Committee?

Mr Bonighton—I do not think that we have ever been before the references committee. The Senate Foreign Affairs, Defence and Trade Legislation Committee is the only committee, I guess, that DSD has come before.

Senator ROBERT RAY—Are you aware that, if any of us want to pursue DSD issues at the Senate estimates committee, we cannot do so in camera?

Mr Bonighton—I am not formally aware of that. I am aware that there is an informal understanding that that would be the case.

Senator ROBERT RAY—Do you think that I would mislead you about it?

Mr Bonighton—Not at all, Senator.

Senator ROBERT RAY—Well, it is a fact that it cannot be done in camera. So I put it to you to reconsider that it would be better to have an experienced committee dealing in intelligence matters with the limited powers that it has bringing you under its purview than saying these other avenues are available, which do not have restrictions, which cannot meet in camera, which any senator or member can attend—well, at least any senator; I do not know what the opportunities are for House of Representatives members.

Mr LEO McLEAY—None, none, absolutely none—that is the trouble.

Senator ROBERT RAY—And, remember, ASIO, ASIS and DIO have all had the odd slash outside the off stump over recent years and have got caught. You have not, but the day will come. And isn't it much better to say, 'Yes, we've made a mistake but we've had a parliamentary oversight—it's partly their problem, too'? Don't you realise that you are much better to be inside the tent than to be outside it? Anyway, I will let you respond to that diatribe.

Mr Bonighton—It is a brilliant argument, Senator, I must say. I guess the only thing that I can say is, as I have pointed out, that we are quite different from ASIS and ASIO in our finance and administration. That is what we are talking about—we are not talking about operations; we are talking finance and administration.

Senator ROBERT RAY—We would also bring in DIO and DIGO; you would not be by yourself.

Mr Bonighton—I will certainly pass the question to my colleague after I have had a go at it, if I may, Senator. I guess I am coming from where I sit, and where I sit is where I stand—that is, I am the one who is going to have to provide the additional data and I am the one who is going to have to provide what appears to me to be another layer of oversight. I am already going through a departmental process, which, I guess you would know from your background, can be somewhat nauseating in its detail—and it may not always be enlightening. That is one point.

The other point is that in our business any publicity is bad publicity. I worry about a further public oversight of our activities. I do not mind revealing failures in camera and I do not mind revealing successes in camera. The irony of our business is that any discussion of what we do is an alerting mechanism to potential targets.

Mr LEO McLEAY—But what Senator Ray is putting to you is a better option. No-one has taken an interest in you in estimates committees up until now. They might start to do that. The alternatives might be that people take an interest at the estimates committee or you deal with this committee, which is required to hear your evidence in camera.

Senator ROBERT RAY—For instance, we do not pursue ASIO much at estimates because we have another, much better alternative.

Mr Bonighton—If I cannot do any better, I will pass to my colleague.

Mr Carmody—All the intelligence output organisations, including DSD, DIO and DIGO, along with the other five outputs in Defence, are subject to a great deal of scrutiny within Defence. The same scrutiny that is applied to every other financial, budgetary and management program within Defence is applied to the intelligence group in the intelligence program. So there is considerable oversight already. There is also the Inspector-General's mechanism, as you know very well.

I understood your point on in camera evidence to the Senate select committee. I am not sure whether the Joint Standing Committee on Foreign Affairs, Defence and Trade is able to take in camera evidence. That committee structure is there for oversight also. My view is that there is already a considerable financial and budgetary oversight of those three organisations.

Senator ROBERT RAY—The moment you bring DSD within an ASIO committee there will not be oversight from the separate Senate committee, the joint committee, the estimates committee or the Public Accounts Committee. They are four committees which have potential oversight at the moment that automatically then cede to a specialist committee. So you are going from four potential oversight committees to one. The one that you are then going to has intelligence specialists who understand the sensitivities and will not throw around code names and all the rest because they do not understand what they are.

Mr Carmody—I understand that. At the same time the activities of DSD and the other organisations mentioned are integral to the activities of the Department of Defence as a whole. I think they differ quite significantly from the oversight for ASIO and ASIS. As you know, the functions of both of those organisations are not quite as congruent with their core portfolio function as these are with Defence.

Senator ROBERT RAY—I think that is true and I think we could concede that, but that in no way relates to what the appropriate parliamentary oversight is. It is absolutely valid that they are not identical to the other two, but it does not mean that they can in any way be exempt from parliamentary oversight. The question we are trying to raise here is: what is the most appropriate parliamentary oversight? You seem to be arguing in your submission for all the existing ones, which we have not triggered but which may well get triggered. That would leave you with far less protection and far more annoyance in terms of interference in your operations than what is being proposed by us.

Mr Carmody—I understand the point. I am not sure I can defend it any better except to make the point that the same oversight that applies to DSD and the other agencies is the oversight that applies to the department as a whole.

Mr MELHAM—Following up on what Senator Ray and Mr McLeay have said, there is another angle to this legislation. What this legislation does for the first time, if it goes through in its present form, is authorise breaches of Australian law to take place and for indemnities to flow. This is a first. What we are also talking about here is the separation of powers: you have got the judiciary and you have got the executive. I think Senator Ray and Mr McLeay are talking about the responsibility and the role for the parliament. We should not be abrogating that responsibility if we let this legislation through. One of the balances is that it is not good enough for the Inspector-General to be technically providing the only oversight of you. If parliament is going to turnaround and allow indemnities for breaches of Australian law because of public policy reasons, there is a role for a specialist parliamentary committee to be in effect asking, 'Who guards the guard while the guard guards you?'

Mr Carmody—If I may try and separate the two issues slightly—

Mr MELHAM—I would argue that you cannot separate them. Sorry, I do not want to interrupt you; I just want you to know where I am coming from. What we are doing is giving extraordinary powers here to the DSD and these other agencies. One of the fundamental arguments from the Council for Civil Liberties and other groups is that this is a really dangerous path to go down. You cannot abrogate totally your responsibility in terms of a continuing monitoring and supervisory role within limits. What Senator Ray is suggesting is that it is in everyone's interest to have a specialist parliamentary committee there as a backstop, rather than these other committees.

Mr Carmody—I understand the point, and I also understand your point about not separating the two issues, but I point out that budgetary and financial oversight is one element of this. We have quite extensive oversight of the way all of the organisations are managed. I believe there is a significant amount of visibility of that, either internally within Defence or externally. The issue of immunities is, I think, certainly very closely related. Mr Bonighton might wish to respond on the process that an organisation would seek to go through when it was seeking to operate under that sort of arrangement, but my understanding is that that is with full ministerial approval. It is therefore an activity which has approval and is under considerable review by organisations such as the office of the Inspector-General, which was set up very much for that purpose and does that consistently and constantly across all of the agencies with a great deal of effect.

CHAIR—On that point, I think we should move on to immunities. What happens if this bill does not go through? How much would the agency be restricted in its activities? As part of laying out the process, which you indicated you would like to do, what sorts of areas would be impinged?

Mr Bonighton—Again this is rather a sensitive area, but let me try and give you a general scenario. We all know that we are in the middle of an information revolution, and that is predicated on the new communications technologies that are abroad in the world. The old days of low volume, wireless communications and morse code are long gone, but that is the sort of environment for which DSD was established. Increasingly in the future we are going to be in a world of infinitely varied and complex communication systems, where the velocity of those communications will be at speeds that would not even be countenanced 10 or 15 years ago and where volumes are exponentially increasing.

DSD's job can be described as looking for nuggets of intelligence in mullock heaps of information. If something like the Cybercrime Bill 2001 went through with its extraterritoriality provisions and without any provision for DSD limited legal liability, we would effectively be cut off from some of those streams of information. It is not that we would go deaf—we would still be able to hear—it is just that we would not be allowed to listen. Given that most Australians would support the sort of capability we have, given proper restraints on what we do, they would be somewhat bemused that on the one hand we have government saying, 'DSD, go out and do a good job,' and on the other hand we have legislatures—not necessarily only Commonwealth but around the country—passing laws that have an inadvertent effect of threatening that very capability. So that is where we are coming from. We are not after a carte blanche. We are after very tailored and specific exemptions. We are after a strong assurance regime that the Inspector-General can effectively police.

CHAIR—For the record, would you run through the process that you would see would do some of those things that you would require?

Mr Bonighton—Central to this is the question of ministerial authorisation and direction. We would want very clearly laid out for the minister, under that section of the bill, exactly what we propose to do over what time period. That has the effect of bringing the Inspector-General into the inspection procedure, because he has to check that what we have done matches those directions. In that ministerial authorisation, we would undertake to set out other sensitive areas that we might be involved in. That would be key to the operation of the legislation.

CHAIR—But, as you said, the point is that it is not carte blanche.

Mr Bonighton—Absolutely not. The thing that is most likely to undermine the legitimacy of DSD is any thought that we are targeting Australian citizens—that we are looking at their communications. That is not our role. Foreign communications is our bag. We have more than enough to do, and we do not want to undermine the validity of what we are able to do. It is a tough business.

Mr HAWKER—Let me follow up on the point you made earlier. In your submission you said:

> In recent years, DSD has been increasingly restricted in its ability to perform its functions by the unintended consequences of Australian laws, particularly where those laws can have application overseas.

You alluded to that a minute ago, but could you expand on that and give us an idea which laws you are referring to?

Mr Bonighton—I can expand upon it in general. I cannot really give you specific cases without going into our capability sources and methods, but there are a number of occasions on which we have sought legal advice before we have undertaken some of our activities. There have been other cases where we have gone to the Inspector-General and sought his advice on what we perceived as grey areas in what we are doing. So it is a real problem today.

Mr HAWKER—Let me come at it from another way. How would you suggest that that might be addressed?

Mr Bonighton—My suggestion is that this bill goes a long way to addressing it.

Mr MELHAM—Through section 14?

Mr Bonighton—Indeed. What we are looking for is a stable and certain environment.

Mr MELHAM—It seems to me that in terms of this power you are talking about it is an authorisation process where you are planning with precision what you propose to do. What I am concerned about is what you would be putting in place. For instance, do you envisage retrospective authorisation?

Mr Bonighton—Whoops!

Mr MELHAM—What is the next step? What I am concerned about is this: what if there have to be on-call decisions made or where they have not had an opportunity to go through a chain of command or whatever? Is that envisaged in this process?

Mr Bonighton—If there were any indication that we had operated outside the law, I would be at the minister's office immediately, and I would be notifying the Inspector-General as well.

Mr MELHAM—I accept that. What I am interested is: what is proposed, because I think we are living in cloud-cuckoo-land if we think that an occasion is not going to come when someone is going to have to make a call and there is not necessarily the timelag to get an authorisation process. What are the protocols that you envisage? Is it going to be part of the authorisation process that we do not do this under any circumstances, so that there is no retrospective indemnity?

Mr Bonighton—If it is not in the ministerial authorisation and we have somebody doing something that is not authorised, then it would be stopped immediately. Then you would go back and inform ministers and the I-G that this has happened. Mea culpa should not happen. If there is something wrong with our processes, we need to change them or we need to do something about the individual who has transgressed.

Senator ROBERT RAY—Where it is authorised and it is then discovered by another authority that there has been a breach of the law, at what point and how do you intervene? Do you intervene with the police, do you intervene with the DPP, or do you run it as a defence in a court case?

Mr Bonighton—I would go the Inspector-General and seek his advice on what the most appropriate course is.

Senator ROBERT RAY—Would you go to the Government Solicitor's office?

Mr Bonighton—I would not go there first; I would go straight to the I-G. He is the guy inspecting my legality and propriety. He would advise me where to go, I would hope.

Senator ROBERT RAY—I do not think that is right, with respect. What we are saying is that there has been a breach of the law in the normal course of your work, under authorised activity, which has come to the attention of, let's say, the ACT police. They start investigating and are thinking of recommending a prosecution. Yet the officer of DSD was operating within authorisation and within the cover of section 14. What do you do to head this off? Do you go to the Inspector-General, do you go to the Federal Police, do you go to the DPP, do you wait for a court case, or do you go to the Government Solicitor's office and get their advice?

Mr Bonighton—I would do two things. I would go straight to the I-G and to the minister.

Mr Carmody—I would not dispute that. I was slightly lost in the two, because I could not work out whether we were dealing with the question of authorisation in advance, where the nature of the signals intelligence business is that Mr Bonighton's organisation would seek to engage in an activity of some sort and seek authorisation in advance. It would be unlikely that, given the nature of that authorisation, it would come across something that had not been anticipated. It would be extremely unlikely. I was trying to make certain that you were talking about that situation and not just day-to-day activities that you are suggesting may well contravene the law. Are we talking about the same sorts of issues?

Senator ROBERT RAY—We are putting the section of the act in to protect officers of ASIS and DSD.

Mr Carmody—Yes, that is correct.

Senator ROBERT RAY—Both organisations are operating overseas, and there is an increasing tendency of legislation to make things an offence not only within Australia but overseas, especially computer related offences. That protection is there for you and for your officers. One of your officers has, in the planning of one of these operations overseas, technically broken the law, and that is discoverable by an Australian law enforcement agency that may not know the person is working for DSD or ASIS. Yet they are protected by this act. What procedures are you going to adopt to deal with this matter? It may well be that you have not thought this through yet. The bill has not gone to parliament, it has not been proclaimed, et cetera. But we are asking you to think it through, and we will be asking the other agency this morning to think it through.

Mr Carmody—I would agree with my colleague. In the first instance, I would certainly go to the Inspector-General, and I would go to the minister and say, 'This is the matter at hand.' That would probably—as you quite correctly put it, I have not thought through all of the issues—move us immediately to the Australian Government Solicitor, but I would certainly make the first two calls the first point.

Senator ROBERT RAY—I know Mr Blick sat at the back. It may be an idea if at some stage we could ask him—and maybe he can come to the table now—whether he thinks it is a good idea to develop a protocol of how you approach these matters with the two agencies. I do not know if he is willing to come to the table now.

Mr Bonighton—Could I perhaps pick up a point after that.

Senator ROBERT RAY—I am sorry to drag you up here, but we will be putting to ASIS later this morning that sort of scenario. How will they deal with this situation? Is it a matter of heading it off with the police, the DPP or actually in the court? DSD this morning said that they think they would come and see you first. ASIS may say the same thing. So do you think you should give some thought to the protocol on how these things are handled?

Mr Blick—I would be very happy to do that. My instinctive reaction is that, if we are talking about law enforcement authorities in the ACT, which we presumably normally would be—

Mr LEO McLEAY—Or DSD anywhere, because they have got stations around other places in the country.

Mr Blick—Yes. The appropriate place to go to get, in effect, the law enforcement authorities told that this is being done under proper authorisation is probably the government, which can then liaise as appropriate with the other authorities within government. I would certainly expect that in the normal course I would become involved at least at the information level from DSD, ASIS or whatever. But, to get back to your first point, yes, I think we should develop a protocol in case this kind of thing happens—

Senator ROBERT RAY—That is good.

Mr Blick—And we will work on that from day one of the legislation.

Mr Bonighton—Perhaps I could just pick up a point on that. We would welcome a protocol. We are after certainty and stability in our environment. On that point about where we should go next if we discovered something like that, the last thing I want in my organisation is 'nudge, nudge, wink, wink, let's go and talk to the coppers and it will be OK'. We need to involve a proper—

Senator ROBERT RAY—The reason you need to involve the Inspector-General is in case it is a 'nudge, nudge, wink, wink' that has not been authorised—

Mr Bonighton—Correct.

Senator ROBERT RAY—That there has been a breach of the law and they are trying to get away with it.

Mr Bonighton—Correct.

Senator ROBERT RAY—That is why the Inspector-General needs to be involved on all occasions, either way.

Mr Bonighton—Indeed.

Mr LEO McLEAY—I go back to Mr Melham's original question, which is about authorisation and after the fact authorisation. As I understand it, all of the activities that you do are individually authorised at a ministerial level. Is that correct?

Mr Bonighton—All the activities that would be described as sensitive are specifically authorised. What is 'sensitive'? This is a bit of an awkward one to answer, but it may be where it might involve liaison with our HUMINT colleagues, for instance. That sort of thing would be individually authorised. In general terms, what we do is brief our minister on what we do, how we do it, where our intercept sites are—the whole bit. But for specific operations we would be briefing him individually.

Mr LEO McLEAY—I think you are getting to the stage where you are giving me a bit of difficulty. If we are going to give you and your officers an indemnity, then I think members of parliament would feel far more comfortable if we knew that that indemnity applied to people who were doing specific things that were authorised at a ministerial level. I think, from what they have told us, ASIS have individual projects that are all authorised at a ministerial level. Sections 8 and 9 of the bill seem to suggest that the activities of these agencies will be individually authorised, that someone, somewhere, at a ministerial level says: 'Go and do this. Go and do that.'

Mr Bonighton—That is exactly what I am—

Mr LEO McLEAY—Are we changing our mind here?

Mr Bonighton—No.

Mr LEO McLEAY—Can you reassure me of this?

Mr Bonighton—No, that is exactly what I want out of this bill. I want a certain authorisation and directions procedure. That would be great for me; it is exactly what I am after. At present, much of what we do is not in contravention of any law. We are not breaking any law. We are trying to future proof ourselves here. We see a significant problem coming up—and I talked about the mullock heaps of information, but that is the problem facing us.

Mr LEO McLEAY—Can you see yourself ever being in the position where you would be trying to get retrospective authorisation from a minister?

Mr Bonighton—No, absolutely not. What is past is past. We look to the future.

Mr LEO McLEAY—If this bill were passed and your officers were granted immunity for carrying out their work, is it foreseeable that an exercise could start without direction or authorisation from the minister and you would then seek retrospective authorisation to protect those people?

Mr Bonighton—No. I would be going to the Inspector-General and saying there had been a transgression.

Mr LEO McLEAY—Thank you.

CHAIR—Thank you very much for appearing before the committee this morning and being so frank. We will obviously be sending you a copy of the transcript. The secretary will be in touch if we need any more information.

[10.01 a.m.]

RICHARDSON, Mr Dennis, Director-General, Australian Security Intelligence Organisation

CHAIR—I welcome Mr Dennis Richardson from the Australian Security Intelligence Organisation. Although the committee does not require you to give evidence under oath, I should advise you that the hearings are legal proceedings of the parliament and warrant the same respect as proceedings of the House or the Senate. The giving of false or misleading evidence is a serious matter and may be regarded as a contempt of parliament. Do you wish to make some introductory remarks before we proceed to questions?

Mr Richardson—I would just make three brief comments. First of all, as stated in our written submission, we are supportive of the proposals in the bill. Secondly, ASIO is not affected by the proposed legislation in the same way as ASIS and DSD. The major impact on ASIO is the establishment of the proposed new joint parliamentary committee, and we are supportive of what is proposed there. Thirdly, while ASIO officers do not have immunities as stated, ASIO does, as you know, have the power under warrant and with proper authorisation to undertake activities which would otherwise be illegal. That is not granting an immunity, but it is part of a philosophy which goes to the need for people in certain agencies to sometimes undertake activity in the proper performance of their functions which would otherwise be illegal.

CHAIR—Thank you. Could I move on to the area of the operations of the new committee. While it is based on the arrangements of the present ASIO committee, there are some differences. One of the specific differences is that the new committee would be required to look at the expenditure and administration of these agencies. What would be your definition of administration or expenditure?

Mr Richardson—It is the totality of the organisation outside of specific operations. But it would nonetheless involve the administration and expenditure of the totality of the organisation's work.

CHAIR—That raises some interesting points because the UK committee, which has evolved over the last seven or eight years, finds that it does sometimes have to delve into operational areas—admittedly, usually past operations. In his submission yesterday, David MacGibbon actually made reference to the fact that there may be a necessity at some time for the committee, when examining expenditure, to get into some of these areas. Do you see any great difficulty in that, or are we drawing too wide a bow on it?

Mr Richardson—My personal view would be that you would take that on a case-by-case basis, and I would suspect there would be times when there would be a difference of view between the committee and government. There could be times when there is a commonality of view and the like. I think it would be difficult to be dogmatic about that up-front. I think it is worth observing that the UK committee is not a parliamentary committee; it is a committee of the parliament appointed by the Prime Minister. I do not know a lot about those things, but there

are differences. Of course, the UK system does not have an Inspector-General of Intelligence and Security with the same oversight functions as the Australian Inspector-General.

Mr LEO McLEAY—In his submission yesterday to the committee, Dr MacGibbon said that he thought the heads of agencies such as yours might be more forthcoming with members of parliament who were on the committee if those members had security clearances. Do you see that as adding anything to the role that the committee could do?

Mr Richardson—Personally, I think that goes to a philosophical issue in terms of the parliament and the way you see it. I think there has been a longstanding position in Australia that members of parliament are not security cleared, and I think that is common in other parliamentary democracies. So if you wanted to change that, I do not think it is an issue for me.

Mr LEO McLEAY—I am glad to hear you say that. Putting it as a more specific issue, would you feel you were able to be more frank with a committee if the members were security cleared, or would you be happy with the way they are at present?

Mr Richardson—Personally, I would interact with any committee of the parliament in accordance with the rules of that committee. If the requirements of the legislation were such that I should interact totally on any matter whatsoever—operations or whatever—then I would do so. That is not a decision for me to take; it is a decision for others to take and it is my responsibility then to operate within the framework you establish.

Mr LEO McLEAY—So a security clearance would be neither here nor there in your mind?

Mr Richardson—Again, I think that goes to a philosophical issue which I think is for other people to address.

Mr LEO McLEAY—But at an operational level?

Mr Richardson—I think it would be wrong on the part of me or anyone else to be interacting with the parliament under rules that they establish in their own minds themselves.

Senator ROBERT RAY—You have been around the track a bit—that is, around this building. Personally, would you prefer to be accountable to the current ASIO committee, an estimates committee going flat chat or a Joint Foreign Affairs, Defence and Trade Committee going full chat? Of the three committees, what would you as director prefer?

Mr Richardson—It does not worry me.

Senator ROBERT RAY—It does worry DSD, though.

Mr Richardson—I have interacted with all the committees, and sometimes it is pretty uncomfortable. On one occasion I spent from 6.30 in the evening until after 12 o'clock at night giving evidence before a committee. That becomes very tough, simply because it becomes very draining trying to concentrate for that period of time.

Senator ROBERT RAY—You are accountable to the same committees as DSD, plus the ASIO committee. Does being accountable to the ASIO committee put a higher workload on you?

Mr Richardson—No, it has not up to this point. I suppose it is fair to say that the proposed new committee has a different remit from the existing ASIO committee, and I think it would be reasonable to assume that the proposed new committee would impose a workload that is not currently there, but so be it.

Mr MELHAM—Mr Richardson, in your submission on page 2 at paragraph 7, you refer to clause 14 in the bill and the provision for limited legal liability in relation to ASIS and DSD functions as appropriate and desirable. You do not see that requirement needed for ASIO in the performance of its operations? That submission reads in a way that, frankly, from ASIO's point of view, it is not really required.

Mr Richardson—We have a warrant arrangement—

Mr MELHAM—I accept that.

Mr Richardson—Given that most of our work is within Australia and we are interacting with the community all the time, what you have put around ASIO is different from what you might put around an organisation, firstly, that is operating overseas and, secondly, that is not dealing with your own community in the way we are. However, the extent to which we need to engage in activity in our own community which would otherwise be illegal, while we do not have immunities we do have a legal framework which enables us to do things with proper authorisation which other members of the community cannot.

Mr MELHAM—I accept that. So you are saying that at the moment what exists is sufficient for ASIO's purposes?

Mr Richardson—Yes.

Mr MELHAM—In other words, ASIO itself as an organisation does not require section 14 as it is currently drafted in this act?

Mr Richardson—That is right. But, if I were heading up DSD or ASIS, I would argue that that was needed.

Mr LEO McLEAY—Mr Richardson, in your opening remarks you alluded to the fact that ASIO does work for other agencies. Could you expand on that a little?

Mr Richardson—We are responsible, under legislation, not only for security as defined in the act but also for the collection of foreign intelligence within Australia at the request of either the Minister for Defence or the Minister for Foreign Affairs. So we undertake work in Australia on behalf of other agencies.

Mr LEO McLEAY—Which therefore gives those agencies access to your warrant capability?

Mr Richardson—That means that any activity being undertaken by the agencies within Australia is being conducted within the legal framework established for ASIO. It means you then do not have two or three different agencies operating within Australia under different legal frameworks.

Mr LEO McLEAY—Is it your understanding that, for these other agencies to do any work in Australia, they must do it through your organisation?

Mr Richardson—There is some work of an open kind that they could do—that is, there is work of an open kind that does not run up against the need for the use of special powers.

Mr LEO McLEAY—What do you mean by that? What does 'open kind' mean?

Mr Richardson—For instance, you do not require legislation—or not up to this point—to run an agent. So you could do certain things with an agent without coming to ASIO. However, if you wanted to search and enter, to access telecommunications, to access data in computer or to undertake any of the functions which require special powers and for which there is legislative cover, you would have to come to ASIO.

Mr LEO McLEAY—So you believe it would be quite within the law for ASIS to run agents in Australia?

Mr Richardson—No, I am not saying that.

Mr LEO McLEAY—Let me rephrase that: in your view, is it within the law for ASIS to run agents in Australia?

Mr Richardson—To avoid going beyond my own knowledge, I think the Attorney-General's Department would be the people to give advice on that.

Mr McARTHUR—I would seek your comment on the relationship between ASIO and the parliamentary committee. It is my understanding that there was some conflict some 10 or 15 years ago. What advice would you be giving to the Director-General of ASIS of your experience and your relationship with the parliamentary committee on this very vexed question of parliamentary supervision of ASIO and ASIS?

Mr Richardson—I would say what I have already said to my colleagues, both privately and now publicly, that is, I think it is a positive move. You should not see parliamentary oversight in terms of being confrontational. It is just part of the system, and you enjoin in it in that way. I do not think you approach it with any particularly negative mindset.

Mr McARTHUR—So, in your experience, you have found it to be a worthwhile relationship?

Mr Richardson—Yes.

Mr McARTHUR—Dr MacGibbon, in his evidence yesterday, went to great lengths to talk about the quality of the committee and security checks, et cetera, in the experience of America and the UK. Do you see any difficulties that might arise in the future between the agencies and the parliamentary committee?

Mr Richardson—I think you will get tensions from time to time, but I think you do now, whether it is an estimates committee or whatever. But that is just part and parcel of the process.

Mr McARTHUR—Tensions on what—in discussions on operational matters?

Mr Richardson—For instance, in Senate estimates, you can get differences on what is policy and what is not policy. You can get tensions in terms of what you think is a fair question and what you think is not.

Mr McARTHUR—But under this bill, you will be relating to this particular committee. Senator Ray has raised the matter of dealing directly with a committee who have some understanding of your role. Do you feel it would be a better way to do business?

Mr Richardson—I suppose I was being a bit delphic. I personally think it is reasonable for there to be a parliamentary committee that has specific oversight in this area.

Mr McARTHUR—How far do you think the oversight should go? That is the key question.

Mr Richardson—That is not for me; that is for the decision makers. It is my job to interact with the committee, as determined by others, and to the extent that I have personal views, they are not personal views that I should be putting on the public record.

CHAIR—The issue of the distribution of criminal intelligence by the agencies has been at the forefront of the hearings of the last couple of days. Could you give us an indication of what ASIO's order is for communicating criminal intelligence to law enforcement organisations?

Mr Richardson—We only come across intelligence relevant to law enforcement incidentally because under the act we can only pursue matters as defined in it. Security law enforcement is excluded from the definition of security. Where, in the performance of our duties, we come across intelligence that is relevant to law enforcement, then we can, and we do, pass that on. Prior to an amendment to the ASIO Act in 1999 we had to pass that material via the Attorney-General, but that amendment enabled us to pass it directly to law enforcement. Secondly, we sometimes, but not very often, receive material from overseas counterparts that can be relevant to law enforcement and we pass that on also.

CHAIR—Are there any further questions?

Senator ROBERT RAY—I do not think it concerns you too much, but would D-notices have any effect on you now?

Mr Richardson—No.

Senator ROBERT RAY—They are basically inoperative and it is best to legislate than to have a D-notice, isn't it?

Mr Richardson—I do not know. I have not been involved in a discussion on D-notices for the last X number of years. It just does not affect me.

CHAIR—If there are no further questions, thank you very much for your attendance here today and, as usual, for the frank way in which you have answered our questions.

Mr Richardson—Thank you.

[10.23 a.m.]

HOLLAND, Mr Keith, Assistant Secretary, Security Law and Justice Branch, Attorney-General's Department

TAYLOR, Mr Allan Robert, Director-General, Australian Secret Intelligence Service

CHAIR—Although the committee does not require you to give evidence under oath, I should advise you that the hearings are legal proceedings of the parliament and warrant the same respect as proceedings of the House or the Senate. The giving of false or misleading evidence is a serious matter and may be regarded as a contempt of parliament. Do you wish to make some introductory remarks before we proceed to questions?

Mr Taylor—Thank you. If I may, I would like to make a couple of comments about the bill. The first one is that ASIS really welcomes the Intelligence Services Bill and the provision in the Cybercrime Bill 2001 relating to ASIS and DSD, and we support them. As you know, the Intelligence Services Bill had its genesis in the report of the commission of inquiry on ASIS which was conducted by the Hon. Mr Samuels and Michael Codd in 1995. Particular benefits were identified by that inquiry in terms of legislation for ASIS, and I think they are still relevant. They are that by continuing ASIS in its existence through placing it on a statutory basis and providing authority for its activities it was following through a desirable principle and it would be of benefit in practice to the agency. It would provide formal public recognition of ASIS's role in serving and protecting Australia's national interests as a foreign intelligence collector, it would provide greater transparency and accountability to ASIS, and it should give greater certainty to members of the public that ASIS exercises its functions properly and responsibly. Moreover, it brings ASIS into line with counterpart agencies in most other Western democracies.

The bill sets out the functions of ASIS and then provides limitations on those function. The functions are clearly related to ASIS's role as a foreign intelligence collector. We are able to distribute that intelligence, conduct counterintelligence activities and liaise with foreign counterpart agencies. In addition, the bill provides for the government of the day to have the option to direct ASIS to perform other functions within strictly defined limits.

The bill places limitations on ASIS's functions. Those functions can be performed only in the interests of Australia's national security, Australia's foreign relations or Australia's national economic wellbeing, and only to the extent that these are affected by the capabilities, intentions or activities of people or organisations outside Australia. These limitations underline that ASIS is a foreign intelligence collector. The bill states that ASIS must not plan for or undertake paramilitary activities or activities involving violence against the person or the use of weapons, and states that ASIS's functions do not include police or law enforcement functions.

The bill also establishes a framework for the authorisation and conduct of ASIS's activities. Central to that is the direction from the minister to the Director-General of ASIS, which must specify the circumstances where the director-general must obtain from the minister authorisations for the conduct of particular activities. This is similar to the current directive, which says when the director-general needs to get ministerial approval.

Under the bill, prior to directing ASIS to undertake other activities under clause 6(1)(e)—that is the flexibility part of the functions—the minister must consult other ministers who have related responsibilities. The minister must be satisfied, before giving authorisation for activities for which authorisation is required, that the activities are necessary for the proper performance of a function of ASIS, that satisfactory arrangements are in place to ensure that nothing will be done beyond what is necessary for the proper performance of a function of ASIS, and that the nature and consequences of the acts will be reasonable, having regard to the purposes for which they are carried out.

In the accountability framework of the bill, the role of the Inspector-General is important. The Inspector-General must receive a copy of the ministerial direction and of any direction to ASIS to conduct other activities, and he must be able to monitor compliance with those directions. IGIS must also be able to view all ministerial authorisations under those directions and ensure that ASIS's conduct in carrying out those authorisations was undertaken legally and with propriety. The other significant part of the accountability framework is the Parliamentary Joint Committee for ASIO and ASIS, based on the general arrangements established by the ASIO committee.

In part this bill places the current functions and arrangements governing ASIS on a legislative basis. It does not add to ASIS's functions, but there are three important respects in which the circumstances in which ASIS operates would be changed as a result of this legislation. They are: greater oversight and accountability, the limited immunities and the protection of ASIS staff. I will comment briefly on those but in reverse order. In terms of the protection of ASIS staff, the bill provides that the identities of staff members of ASIS are to be protected, and it is a similar protection that is afforded to the staff members of ASIO under the ASIO Act of 1979. This is the first time that ASIS staff have had this legal protection, and it is important for the secure conduct of ASIS activities.

In terms of the limited immunities, in recent years ASIS has been restricted in its ability to achieve the objectives of government due to developments in technology, especially the holding of information and data electronically and the increase in Australian law with extraterritorial effect. These two developments have already led to situations where ASIS has not been able to collect intelligence, and this trend is expected to continue. The Cybercrime Bill 2001, which includes limited immunities for ASIS and DSD, is an example of the proposed legislation, which covers modern technology and which would have effect outside Australia.

A further example of the application of Australian laws overseas relates to conspiracy. In certain circumstances, even planning a foreign intelligence activity in Australia to take place overseas could be in contravention of Australian law. These limited immunities do not override any of the restrictions on ASIS's functions in the bill, including the prohibitions on the use of weapons, violence and paramilitary activities, and they would only apply in the course of properly sanctioned and performed activities as set out in the bill. ASIS would not have open season to break the law, and the immunities are necessary for ASIS to perform its functions fully. Activities involving limited immunities will of course be subject to close scrutiny by the Inspector-General, as are all ASIS activities. The Inspector-General has access to all ASIS operational files and, as I have already noted, monitors the legality and propriety of ASIS activities.

The third main category of change for ASIS is the establishment of the parliamentary joint committee. That is central to the new accountability framework, and it is welcomed by ASIS. The committee would have, among other things, a statutory mandate to review the administration and the expenditure of ASIO and ASIS. As a result, its responsibilities, as I understand it, would be broader than those of the current ASIO committee.

The Samuels inquiry found in 1995 that ASIS's accountability and oversight arrangements were comprehensive and effective. The combination of IGIS's continuing monitoring, the proposed parliamentary joint committee's review of expenditure and administration and the ANAO audit, which now includes all operational expenditure of ASIS, further strengthens these arrangements and enhances their transparency. Overall the bill brings together desirable oversight and essential accountability while maintaining the secrecy which is necessary to protect operations, sources and staff, which must be done if ASIS is to be viable.

CHAIR—Thank you very much indeed. Just as I did with Mr Richardson, in terms of the operations of the new committee, could you give us a definition of what you might regard as the administration and expenditure aspects of ASIS that the committee may be responsible for or may be able to investigate?

Mr Taylor—I think it would cover the whole gamut of administrative and expenditure: finance matters, personnel issues—anything that comes in that category. I suppose another way of looking at it is to say that it would cover everything that is not specifically ruled out in the bill itself. I would imagine that the committee itself would have ideas on how it could look into the administrative and expenditure side of ASIS and that in the course of the committee's hearings that would develop. My understanding of how the UK committee, which is the one perhaps nearest to this model, works is that over time the relationship between the committee and the agencies has developed and trust has developed, and the whole business has proceeded on that basis. I would expect that to be a similar case here. I would not like to define it precisely except as it is in the bill, but obviously there is room there for cooperation—and if I could underline that in its approach to the committee ASIS has a very positive and cooperative approach in mind.

CHAIR—In your introduction you made reference to what ASIS is, the activities it is involved in and what it is not involved in. Just for the record—and I do not do this in a silly sense—what would be your definition of paramilitary?

Mr Taylor—Quite simply, activities which involve the use of any armed military-like units or personnel to conduct particular actions.

CHAIR—Thank you for that.

Mr LEO McLEAY—Mr Taylor, clause 6 of the bill outlines the functions of ASIS. Could you tell the committee whether the functions and responsibilities outlined in clause 6 are any different from the current ministerial directive that you have? Has anything been added or is anything that is in the current directive not there?

Mr Taylor—No, they represent the functions of ASIS as set out in the directive, with one exception, which may fall into the category of activities that could come under 6(1)(e). ASIS

has authority to work against people traffickers: that was agreed by the government and added to the directive. But I think the way in which the functions are there defined reflects the current situation: 6(1)(e) reflects the fact that now government has the power to direct ASIS to carry out activities and that power to change the functions of ASIS by adding to them in that specific and limited way is protected in 6(1)(e) to meet any contingency that might arise in future. It is an attempt not to tie the hand of government in any contingency which might arise.

Mr LEO McLEAY—In relation to some of the things that might occur with the provision of these immunities—and you might have heard me ask Mr Richardson this question—is it lawful for ASIS to run agents in Australia?

Mr Taylor—ASIS's activities in Australia are conducted only insofar as they are in accordance with Australian law, so we would not and do not break Australian law. We are able to talk to people in Australia, clearly.

Mr LEO McLEAY—That is not the answer to my question. If you do not want to answer the question, you can say that, but the question was: is it lawful?

Mr Taylor—Put another way, if there are agents and we are a foreign intelligence collector and if people who are providing us with foreign intelligence come to Australia or are in Australia, then, provided we are not breaking Australian law, yes, we can deal with them.

Mr LEO McLEAY—Is it lawful for you to recruit agents in Australia?

Mr Taylor—I would give you the same answer: if, in doing so, we do not break Australian law, yes. I know I am being a bit circular. We are a human intelligence organisation that collects intelligence from human sources. Provided we are acting within the law in Australia, we can have relationships with our human sources in Australia.

Mr LEO McLEAY—My understanding is that you would not be able to recruit an Australian citizen to act as an agent within Australia.

Mr Taylor—We do not target Australian citizens in terms of seeking intelligence about Australians. However, if an Australian were able to work for ASIS, that is fine.

Mr LEO McLEAY—So it is lawful for you to recruit an Australian citizen to act as an ASIS agent to gather material for you in Australia?

Mr Taylor—It is not our role to gather material in Australia unless it relates to the capability or intentions of persons and organisations outside Australia—foreign intelligence.

Mr LEO McLEAY—But it is lawful?

Mr Taylor—If there is an Australian in Australia who is prepared to assist ASIS and we are in touch with that person and that person has information relevant to the functions of ASIS, provided we do not break the law in doing so, yes, it is. It would be a meeting—just sitting down and having a cup of coffee with someone.

Mr LEO McLEAY—But if one of those agents carried out an activity in support of their role in gathering information for ASIS, would they then attract the immunities in section 14?

Mr Taylor—Section 14 refers to 'staff member'. My understanding is that that is not the case. In any case, ASIS is not authorised to break the law in Australia. Where ASIS would like to obtain foreign intelligence in Australia, we go through the process of getting the Minister for Foreign Affairs to write to the Attorney to seek a warrant for ASIO to carry out an operation under the ASIO Act. That is for the particular types of activities that ASIO is able to do under its act. I do not think the question arises—as far as I can foresee—that you envisage.

Mr LEO McLEAY—I was asking the question about agents and I was then going to ask you a question about intelligence officers. Noting that a staff member is an intelligence officer and an agent is an agent, section 14 could be read to show that a staff member—that is, an intelligence officer—or an agent is not subject to civil or criminal law in Australia for an act done in Australia in support of or otherwise directly connected with overseas activities. I wanted to know whether there is a separation between ASIS agents and intelligence officers carrying out activities in Australia other than planning activities. Is it your understanding that, under your act and under the changes that this bill can make, ASIS agents or intelligence officers can act in an operational fashion in Australia in support of an ASIS objective overseas, break that law in Australia and be accorded the immunities provided in section 14 of this bill?

Mr Taylor—Planning is the main one which you mentioned, and which I mentioned in my opening statement—

Mr LEO McLEAY—I have no problem with the planning; I am talking about an operational—

Mr Taylor—Where there is a territorial nexus between a jurisdiction in Australia and a jurisdiction overseas, there may be a situation in which doing certain things related to an overseas operation would not be possible without the immunity. In my knowledge, they relate specifically to computer activities.

Mr LEO McLEAY—So ASIS agents could, in support of an overseas operation, operate in Australia, break the law and achieve these immunities?

Mr Holland—I am the Assistant Secretary of the Security Law and Justice Branch in the Attorney-General's Department. We have been involved in the drafting of this legislation. I think part of the confusion that might be arising in this section arises in the understanding of precisely what it is that may or may not be illegal activity in Australia. In the context that you first raised this issue—that is, agents in Australia—there is nothing that would prevent a foreign person who might be used as an agent in Australia handing over information. It is not illegal to hand over information from a foreign country in Australia. So the activities that would be involved there would not need this immunity. In the context of getting that information, there might be an operation planned and things done in order for the activity that would flow from that to take place offshore. In that context, if the activity that was being contemplated was an offence in that country and in Australia, then you would need the immunity. That is the point.

Mr LEO McLEAY—Let me put this another way. Section 14(2) says:

A person is not subject to any civil or criminal liability for any act done inside Australia if:

(a) the act is preparatory to, in support of, or otherwise directly connected with, overseas activities ...

If an ASIS agent or an ASIS intelligence officer in Australia breaks an Australian law in pursuit of a properly authorised objective overseas, is it lawful for that agent to do that? If it is, would that agent be covered by the immunity?

Mr Holland—If I understand your question correctly, the short answer is yes. The parameters of this provision are very precise and contained in the section that you read out—that is, it has to relate to a function of the organisation and it has to be a properly authorised function of the organisation and the activity is directly related to what is going to happen offshore. We have looked at this in the context of planning the operation. Without going into too much detail, there might be other things that might be required to be done. The provision says that, if an officer of the organisation, in the proper performance of their functions, engages in an act that might otherwise attract civil or criminal liability, it will not in those circumstances attract it. It is very narrowly defined because when this provision was being drafted we were very conscious of the fact that, if the provision were drawn too widely and this matter came to judicial interpretation, the courts would read it down. So it was structured in such a way that it was focused specifically on the officers, the agents, the activity that was authorised and the functions authorised by the act.

Mr LEO McLEAY—Let us get it clear here. Section 14 is not just authorising people to do things overseas that might get caught up in the outreach of an Australian law; it is also giving them immunity for breaking a law in Australia.

Mr Taylor—But it is not open season, as I said. ASIS officers cannot just go out and break the law in Australia.

Mr LEO McLEAY—Explain to me why they cannot.

Mr Taylor—For the reasons that Mr Holland just mentioned. If there is a need in the operation to break an Australian law, that must be agreed through the proper processes. It must be in terms of an activity that is clearly in accord with the limitations placed on that in the act. You cannot just go out onto the street and break the law and then claim immunity because you happen to be working with ASIS.

Mr LEO McLEAY—This is the sort of thing that is central to one of the worries about section 14. I think that to try and close off as many of those worries as possible is a sensible thing to do here today. If ASIS were running an overseas operation that required an ASIS intelligence officer, in an operational matter, not a planning matter, to break a law in Australia, what actions would the organisation take about that? Rather than have the officer break the law, would you contract that matter out to another agency who might be able to do it in a way that would not break the Australian law, or would you get an authorisation from the minister or some higher authority that says, 'Yes, this is a sanctioned operation,' or would the person just say, 'We have got a proper overseas operation going. To act in support of that operation, I have to break this Australian law and therefore I have got the immunity covered by section 14'?

Mr Taylor—If that situation arose—and I am trying to think of circumstances where it would, and where it would not be our practice to go to ASIO and do it through the ASIO warrant system—that would certainly need ministerial authorisation. I am trying to envisage a situation where that might happen, and it would relate to—

Mr LEO McLEAY—If you can tell me that it will not happen, that is terrific and we can close the issue.

Mr Taylor—Well, it might happen. How shall I put it? If there is an operation going on overseas and someone involved in that operation visits Australia and needs to have access to the information from that operation, it may be that it comes up against one of the state or territory laws. We would have to look at that very closely to see whether that was something that would require a warrant through ASIO or whether it would be done under this act. It would probably not be something that could be done by ASIO, if you see what I mean. It is hard to go into detail on this, but—

Mr LEO McLEAY—But if that happened, you would seek the sanction of the minister to do it?

Mr Taylor—Yes. I certainly would. It would happen so rarely. The case of breaking Australian laws in a way that was not covered in the conspiracy provision might come up more often as a result of the territorial nexus, which would mean that Australian law extended beyond Australia and that it was being broken overseas. That is where the real problem arises in breaking Australian law.

Mr LEO McLEAY—I understand that. It is this little window of: what can ASIS do in Australia, in an operational rather than a planning sense, with immunity from Australian law?

Mr Taylor—It depends. Without getting into detail, which is difficult for me—

Mr LEO McLEAY—I understand that.

Mr Taylor—It is a small area and, as I indicated, to my knowledge it could relate to something as straightforward as listening to a tape.

Mr MELHAM—You recall the Sheraton Hotel incident, which was the subject of an inquiry?

Senator ROBERT RAY—They are not allowed to do that.

Mr MELHAM—I appreciate that they are not allowed to do that in terms of covert operations or whatever, but there was, for instance, a training exercise where staff and guests were threatened and property was damaged. Could you envisage something like that in the future, and would that attract the immunity provisions of clause 14(1) or (2)?

Mr LEO McLEAY—An agent or intelligence officer could be involved in something as simple as a common assault in Australia while in pursuit of some genuine operational matter to do with a big overseas operation.

Mr Taylor—I cannot imagine that happening. In fact, under the act it cannot. We are not allowed to use violence. It is ruled out. To go back to the question on the Sheraton—

Mr LEO McLEAY—So, if someone used violence, they would not have access to the immunity in clause 14?

Mr Taylor—That is right. They would not. In my view, as director-general, they would not because violence is specifically ruled out in the bill as a limitation on our function.

Mr Holland—If I might intervene here for a moment, Mr Chairman. It is not just the functions that we have to look at in terms of this immunity but the act as a whole and the other provisions and, as the director-general said, that relates to the prohibitions that are there. The act does not just say what can be done; it also says very specifically what cannot be done. The sorts of things that you were referring to come within that category.

Mr LEO McLEAY—That was an example. Do not think that that is the only thing I am talking about.

Mr Holland—No. I think it is also worth saying, and I am sure the director-general would agree, that ASIS does not set out to break the law. To set out to break the law is not its purpose in Australia. Therefore, the sorts of activities that are prohibited would not attract this immunity.

Mr MELHAM—So any immunities that you would be seeking would pre-date the event? You would not see any post-dating of immunities, given that some circumstances might arise that are unforeseen?

Mr Taylor—If that were to happen we would try and get the approval for the situation. If we were faced with something like that we would do it. Where we have come up against this issue, we have taken legal advice. And when the legal advice has been that it would be unlawful, we have not done it.

Mr MELHAM—Do you see this section as necessary in terms of your future operations?

Mr Taylor—Yes, I do.

Mr MELHAM—Without this section, you would see yourself as severely constrained?

Mr Taylor—For that sort of area which, as I mentioned, is coming up more regularly now as a result of the technological changes and the extraterritorial application. I will just go back to the reference to the Sheraton for a moment. That sort of activity was taken out of ASIS's functions as a result of the Sheraton, at the time of the Hope commission, and we have not looked at that at all. It is not something that ASIS would want to do.

Mr MELHAM—But it is the principle that I am concerned about. That was an authorised operation. It was a training exercise and it went wrong, so to speak. Surely the same principles could apply to you in the future: you could plan an exercise and something might go wrong?

Mr Taylor—But we do not plan that sort of exercise, because that is the type of activity that we now cannot do and do not want to do. Our training is very carefully controlled and is done with the full knowledge of the local authorities.

Mr MELHAM—So, from your point of view, any indemnity that you would seek would be something, in terms of your protocols, considered part of a planned operation; it is something you would require beforehand, not after the event?

Mr Taylor—Yes. Certainly before authority were given for an ASIS officer or agent to break Australian law, there would have to be a decision taken to do that.

Mr MELHAM—So you cannot envisage a situation where an on-call decision needs to be made by a particular officer at a particular time that would subsequently require ratification or authorisation?

Mr Taylor—We do very careful planning for what happens overseas. That situation might occur overseas, and it might occur through ignorance because of the extent of some of these provisions.

Mr MELHAM—Would you see the need for the development of a protocol in instances where officers or agents might have to make an on-the-spot decision in relation to something that was unforeseen? Unforeseen circumstances are what I am interested in. How are they to be resolved? Is it something that you would report? For instance—and I think this question was asked of earlier witnesses—is this something in which you would involve the ministry or the Inspector-General post an event?

Mr Taylor—If you are talking about a claim against an ASIS officer for breaking the law that is one thing, and I am happy to come to that.

Mr MELHAM—Even pre the event.

Mr Taylor—We are talking mainly about overseas issues because that is where most of our operations are. I perhaps should give you the sense of our work: most of our operations are mundane. It is meeting people; it is not film stuff.

CHAIR—There is not much Ian Fleming in it?

Mr Taylor—There is very little; it is mundane. Meeting people and collecting intelligence is basically what it is. There are other things, but that is the bread-and-butter work that we do. That is all straightforward and there do not seem to be any legal problems in that. If we anticipate anything that could break Australian law, we seek approval for it. If in the course of an operation something happens that was unexpected and it was thought to be against Australian law, we would seek to rectify that quickly. Once this act comes into place, we will have an education program going through ASIS to ensure that everyone understands precisely

what the immunities, if they go through, mean and what they mean for them. If something were to happen and we learnt about it, we would immediately go to IGIS and seek to ensure that we did what was necessary then.

Mr MELHAM—In that regard do you have a problem with an automatic reporting mechanism to IGIS, for instance, post the event?

Mr Taylor—No. In fact, we do that anyway. If we have any legal issues we have two avenues: (1) we go for legal advice and (2) we discuss it with IGIS.

Mr MELHAM—But I am talking now about this authorisation. Let us say the legislation goes through with clause 14 as it is, do you have any problems with IGIS being automatically notified where authorisations are given after the event?

Mr Taylor—Under the bill, IGIS has access to all the authorisations and monitors them. That is part of the bill and he or she—but he at the moment—is given copies of the directions. He has access to everything.

Mr MELHAM—But do you see any further requirements in terms of resources? Do you see that this would require more resources for IGIS?

Mr Taylor—That is a question you would have to ask him. I do not know. I am sure he wants more resources. The second part of that issue is if an officer is accused of a crime in Australia, for example—

Mr MELHAM—Or if it is brought to your attention that they have transgressed. There does not necessarily have to been a complaint made. What do you envisage would be the protocols if someone transgressed without authorisation? There are obviously different levels of transgression.

Mr Taylor—If we take a hypothetical case: say someone makes an allegation in Australia that X is transgressing the law, does not say that X is an ASIS officer and the police go and talk to X. If X is an ASIS officer—and assume for this case that it is a he and he is—under our current rules within ASIS, X must get in touch with the head of our security and report that. That is in our current processes. At that stage, we would get legal advice from the AGS and seek to bring in the government lawyer, who would then talk to the senior police in that jurisdiction to ensure that they knew what the circumstances were. We would also get from the AGS some idea of whether that person was or was not breaking the law in terms of the bill. We would then go to the minister and inform him of what had happened and to seek his approval for what was going on.

There would be two ways we could go from there. If there was a consideration that the officer had broken the law then, in accordance with our current practices, we would advise that officer to seek legal advice and we would advise the police to pursue it, as they should. The basis of our approach to all of this is that an ASIS officer should be treated like any other Australian under Australian law. If the decision at that stage was to say, 'You have to go through with it,' our role through the use of the AGS would be to protect the Commonwealth's interests in that, which would be basically the name and the affiliation of the officer. If the police wanted to go

ahead with the case, it would then go to the DPP. I imagine, at that stage, the AGS and a senior ASIS officer would fill the DPP in and the case would go to court. That is how that situation would progress under our current procedures. If, however, it was found that we thought he was within the law and the police were not convinced of that and wanted to go ahead, we would prepare a defence for that. But it would still go through the judicial processes.

Mr LEO McLEAY—I want to clear up something from before. I will give you two examples that might better clarify things for me: if an ASIS operative in support of an overseas operation illegally accessed a computer in Australia, would that be operationally legitimate and would that person have the protection of section 14 of this act?

Mr Taylor—I can give you two answers on that. Again, it would depend on the circumstances. It is more likely that that is the sort of operation we would seek to do through an ASIO warrant or seek to have ASIO do. If that is not the case, then it would depend on all the sorts of things that Mr Holland mentioned—whether it was a properly authorised act in terms of a proper performance of ASIS functions, with all the limitations and within the framework envisaged in the act. It is not something that an ASIS officer can go out there and simply—

Mr LEO McLEAY—The way I understand you have answered that question is that the answer is yes. Is that right?

Mr Taylor—No, it is not. I am sorry if my answer was not clear.

Mr LEO McLEAY—I need to clarify in my mind why ASIS cannot—

Mr Taylor—An ASIS officer cannot go out and access a computer just like that. That would not be legal.

Mr LEO McLEAY—My question was: can an ASIS agent, in pursuit of an overseas operation of ASIS that is duly authorised, properly ticked off everywhere, illegally access a computer in Australia and seek the immunity provided in section 14?

Mr Taylor—If that proposal came to me for a decision now, I would be immediately talking with the Director-General of ASIO about the parameters that that sort of operation involved.

Mr LEO McLEAY—That puts you on the side of the goodies. Can the man from A-G's tell me whether or not it is illegal?

Mr Taylor—Whatever happens, you have to have proper authorisations.

Mr Holland—I think the point you are making is that, assuming that all the authorisations have been approved, assuming that they are acting in the lawful course of their functions, the answer would be yes.

Mr LEO McLEAY—My second question is: if, rather than accessing a computer, the agent is accessing an office that he is not authorised to be in, which might be a break and enter or a trespass—

Mr Taylor—If he is not authorised to be there, then he is breaking the law.

Mr LEO McLEAY—What about an office where that person should not be—and they may have got into it by a break and enter or they may have just trespassed when the door was open—an office that was not their office but an office related to their gathering material in support of a properly authorised overseas activity? If they broke the law in Australia in that fashion, would they get immunity under section 14? Are they able to do it, and do they get immunity?

Mr Holland—If the circumstances that you propose arose—and I think that would be highly unlikely in light of what the director-general has said, but in the event that that did occur—yes, they would. But, as we said, it has to be directly connected to the activities overseas.

Mr LEO McLEAY—An overseas operation?

Mr Holland—Everything else that is involved.

Mr MELHAM—They have to be properly authorised; they cannot just go willy-nilly and start hacking into stuff.

Mr Taylor—That is right.

Mr LEO McLEAY—I understand that.

Mr Taylor—ASIS is collecting foreign intelligence and, fundamentally, we work overseas. I can see where you are coming from; I understand the questions.

Mr LEO McLEAY—You have drawn up this legislation, not us. You might say that section 2(a) is very narrow, others would say that it is rather wide; a person receives immunity if the act they do in Australia is preparatory to, in support of or otherwise directly connected with something overseas. That can cover a whole gamut of things that an ASIS staff member or agent can do.

Mr Taylor—But only if it fits all the other parts of the act.

Mr LEO McLEAY—If the minister authorises a very significant intelligence gathering operation in Kashmir and the agent or the person who has a lot to do with that target in Kashmir is an Australian citizen living in Melbourne, to support that operation you might want to look at those things that that person is doing in Melbourne. If you did that at present, you could be in trouble. If this act is passed, you get the immunity.

Mr Taylor—If that person in Melbourne had knowledge that would fit into the type of information that we were seeking about the intentions, capabilities and so on in that country, we would require authorities to do that. The type of information that we are seeking would not be—as far as I can see—held by a normal person living in Melbourne, if you see what I mean.

Mr LEO McLEAY—You obviously have not been to Melbourne recently!

Mr Taylor—I do not know about that.

Mr LEO McLEAY—I am staying away from Sydney, because I go there all the time.

Mr Taylor—What I am trying to get at is that the type of information that we are looking for is quite specific in the definitions in the bill. It is the intentions and capabilities of people and organisations overseas. I cannot imagine where we would want to do that type of operation and, in any case, I am sure that is one that we would not go through with. It would be one where we would look at the possibilities. If it were something that had to be done, we would look at the possibilities of seeking an ASIO warrant. Whether or not it fitted into that, I am not sure.

Mr Holland—Mr Chairman, can I assist the committee a little here? I think it is also worth while looking at this in the overall context of other examples of this. What is being proposed here is not dissimilar to the sorts of indemnities that are given to state, territory and federal law enforcement agencies who, in the course of their activities, may have to break the law under certain circumstances. What then happens in state, territory and federal legislation—and certainly controlled operations are an example of that—is that AFP officers are allowed to be in possession of drugs, which otherwise would be unlawful, except in the defined circumstances within the legislative framework. That is precisely what is happening here, where you are saying, 'Okay, we're setting out what you can and can't do. If you're acting in accordance with the legislation, in those circumstances—and only in those circumstances—having fulfilled all those requirements, this indemnity cuts in.'

CHAIR—Could I now move on to the area of ministerial directions and authorisations? Clauses 8 and 9 set out all the procedures that are there. Are you happy with the way those procedures work? The other thing that I would like to take up is the comment that you make about the need for a classified directive. What is the major difference between a ministerial direction and a classified directive? Is the scrutiny process the same?

Mr Taylor—I think we are talking about the same thing there.

CHAIR—Precisely.

Mr Taylor—I think the point is that, because the ministerial direction will need to set out activities that relate to sources and methods, some of the direction will include that it will need to be classified. That is the point.

CHAIR—So there is absolutely no difference?

Mr Taylor—Between those terminologies, no—not in my mind. The reason that we refer to direction and directive is that the current directive we have is called a directive; the bill talks about a direction. That is where the difference in terminology comes from. It is the same thing. At the moment, the directive includes quite a lot of the administrative arrangements for ASIS which are now included in the bill.

CHAIR—All right.

Mr Taylor—To answer your question, yes, I think the ministerial direction process with the authorisations is a good one. It reflects very much the current situation, which I think works well. In the directive that we have at the moment the minister sets out categories of activities that he wants to specifically authorise. It instructs the director-general to obey Australian law and it instructs the director-general to ensure the proper administration and running of operations. Where there are operations that are not in those categories, they are approved by the director-general but by no-one else. It is the director-general or the minister who must approve an operation.

Mr HAWKER—This may just be in the wording, but in relation to the question of briefing the Leader of the Opposition, under the ASIO Act, as I understand it, there is the point about consulting regularly with the Leader of the Opposition in section 21. It says that you may, with the authorisation of the Prime Minister, brief the Leader of the Opposition. I am just wondering why there is a difference between the ASIO provisions for dealing with the Leader of the Opposition and the ASIS one.

Mr Taylor—My understanding is that Samuels looked at this issue. Samuels recommended that the provisions in the Intelligence Services Bill should be the same or reflect the same situation as in the ASIO Act. As you have pointed out, they are different now. The then government that looked at the Samuels recommendations first back in 1995 rejected that recommendation to have the briefing on the same basis. In the statement the then minister gave on the recommendations of Samuels he made the point that ASIS was in a slightly different situation from ASIO in that ASIO dealt with domestic matters and was highly political, whereas ASIS was mainly concerned with overseas issues and so on and that the practice had developed that the briefing of the Leader of the Opposition be at prime ministerial discretion. That was accepted by the then government and carried over to the current bill. That is the reason. It was looked at originally, accepted by the present government and incorporated in the bill—so that is the difference.

Mr HAWKER—In practice, would that mean that because of the different sensitivities this would be the logical way to go, or is there a lesser need for the briefings to be on the same basis?

Mr Taylor—It is obviously a policy decision. The then minister in 1995 said that, while a statutory right to briefing was justified in the case of ASIO, there was less justification for it in the case of ASIS because ASIS had far less potential to affect the civil rights of Australians or to conduct activities with domestic political implications and ASIS was an agency of government subject to ministerial responsibility and control. The decision then was that the existing formalities and procedures, which were the ones that are now incorporated in this bill, should be maintained. That is the reason. I would have thought that there would be less need to brief the Leader of the Opposition on ASIS because it does not impact domestically, but in terms of briefing the Leader of the Opposition I have no problems with that as director-general. It is just the way it is done, and that is a political decision or a policy decision.

Senator GREIG—In your preamble and in your submission you advocate support not only for the ASIS Bill but also for the Cybercrime Bill. I want to explore a little of the latter. Wearing my other hat as a member of the Senate committee that is looking into the Cybercrime Bill, I am aware that the vast majority of submissions from people in the IT industry and people involved

in computers are scathing in their criticism of that legislation, not because they are opposed to it but because they want to see quality, effective cybercrime legislation, not the bill that has been presented, which they argue is inadequate and unworkable. Why would ASIS, in that context, offer unqualified support for the Cybercrime Bill?

Mr Taylor—Our interest in that bill is solely in the clause that relates to the immunities for ASIS and DSD, and it arises from the fact that the bill has an extraterritorial effect.

Senator GREIG—Do you envisage therefore that ASIS could or should be involved in the search for people involved in computer cracking or hacking based overseas? Is that a part of where you are coming from?

Mr Taylor—No. We do not have any responsibility—that is made clear in the bill—or functions that relate to law enforcement or policing. Ours is a very narrow interest in that bill and it relates solely to the fact that it gives the offences extraterritorial effect.

Senator GREIG—I understand that, but is there the opportunity for a ministerial directive for ASIS to inquire into people overseas who may be involved in Internet cracking or computer hacking?

Mr Taylor—It would not fit into the functions as defined at the moment. It is not the intention of organisations and so on outside Australia. Are you talking about Australians or foreigners?

Senator GREIG—I am talking about both.

Mr Taylor—If there are foreigners and other governments and so on with intentions to damage Australia's national interests and if that fitted into the collection priorities that we had—not in a criminal sense, but in a national security sense, like the capabilities of another organisation or group outside Australia to hack into Australian government things—that might be of interest to ASIS, but that is not the focus of our interest in this bill. That issue would be picked up in the priorities that are determined for ASIS through government procedures for setting the priorities for our intelligence collection, which are not done by ASIS at all; they are done by a government process.

Senator GREIG—Would that not include, for example, a clever individual based overseas who might attempt to break into an Australian based computer network that might be attached to the Australian government?

Mr Taylor—We have not been tasked to do anything like that, no.

Mr LEO McLEAY—Clause 14 confers upon ASIS staff members and agents an indemnity in respect of breaking Australian law in the proper performance of their duties. Mr Taylor has told us that part of the proper performance is that they have to get ministerial authorisation for starting those actions. Could you refresh my memory about where the minister obtains his or her immunity in respect of authorising an action that could result in a breach of Australian law?

Mr Taylor—The minister is defined as a person.

Mr Holland—That was looked at in the drafting of the bill. The minister is a person.

Mr LEO McLEAY—The minister is usually a person. Does the minister pick up his indemnity in clause 14(2)?

Mr Holland—That is correct.

Mr LEO McLEAY—You are now widening clause 14(2) rather remarkably, aren't you? Clause 14(2)(a) refers to a staff member or agent of an agency, and in this case we are talking about ASIS. Do you say that, if the minister picks up the minister's indemnity in clause 14(2) by being a person, all sorts of other persons other than ASIS agents could be indemnified in respect of these activities?

Mr Holland—No.

Mr LEO McLEAY—Why does it say 'a person' rather than 'the minister'?

Mr Holland—In answer to your question, that is correct, but the minister and any other person who might be involved in the activities preparatory to the activities that are taking place offshore would gain indemnity under here. I think that is right.

Mr LEO McLEAY—I think you just told us you were the person who drafted this legislation. In your mind, when you were drafting it, who were these other persons?

Mr Holland—I was not the person who drafted this legislation. My introduction said that my branch was 'assisted in the drafting of this legislation'.

Mr LEO McLEAY—In assisting in the drafting, who were these other persons who may have been in mind?

Mr Holland—I am not in a position to answer that question. In the discussion we are having, we are looking at it in the context of other people who might assist officers or agents of ASIS in actions preparatory to the activities carried out overseas.

Mr LEO McLEAY—So who are they? This also refers to 'in Australia'. These persons could be persons in Australia.

Mr Taylor—I suppose we are talking here about people who may be advising ASIS on a particular issue if one were to come up in relation to the activity. It is this complicated conspiracy problem.

Mr LEO McLEAY—We go back to my original worry about this: in my reading of clause 14—and I am not a lawyer, so I can be excused—I thought the persons referred to in 14(2) were staff members or agents of the agency, as the first line of 14(1) says. I have no problem in giving immunity to staff members or agents of the agency—after we talked about this—but if you are now telling me that subsection (2) relates to any person who has anything to do with ASIS, that they can climb on board with this immunity, I am starting to worry. Who are these

persons? I am quite happy for the minister to be indemnified and even you, Mr Holland, if you had something to do with it.

Mr Taylor—That is right. That is what we are talking about, I think. I think we are talking about people who might be giving advice on an operation. We may talk to another department about the implications of something.

Mr LEO McLEAY—Or could they be persons who are operationally involved?

Mr Taylor—No.

Mr LEO McLEAY—Tell me why they are not—because looking at that it appears that they could be.

Mr Taylor—If they were involved in the operation, yes they would be.

Senator ROBERT RAY—Let us have a look at pages 2 and 3 of the bill, under 'Definitions'.

Mr Taylor—It is:

(a)an Australian citizen; or

(b) a permanent resident.

Senator ROBERT RAY—No; you have a definition of an 'Australian person' but Mr McLeay is making the point that 14(2) refers to 'person'. 'Person' is not defined here. Surely section 9 is where the minister's protection is under ministerial authorisation. Isn't that his protection? It does not rely on 14(2) at all.

Mr Holland—My understanding is that in fact it was intended that the reference to 'person' did pick up the minister. That was certainly my understanding of what I heard when I came into this.

Senator ROBERT RAY—We would not object if 'person' equalled 'minister'. Mr McLeay wants to know, and so do the rest of us, if 'person' equals 'others', who are the others?

Mr LEO McLEAY—If the others are only staff members and agents—

Mr Taylor—I understand the point, and I think we will need to get a specific reply to that.

Mr MELHAM—That is why, as Senator Ray says, my initial reading was that the minister's protection comes from section 9. It talks about—

Mr Holland—Authorisations and so forth. But in terms of the whole lot there was seen to be a gap, as I understand it, and therefore it was thought that that reference would pick up the minister. I think that is right. I will certainly check that and if there is a problem with that then I will let you people know.

Senator ROBERT RAY—That creates a bigger problem for us. What you have done is to go back to the act, pull out the word 'person' and say that the minister is covered. For us, that is a worse explanation because we then want to know why the word 'person' was ever put in. I would understand if 'person' was put in to protect the minister, but if the word 'person' was there before you came to that rationale about the minister I am more worried about it.

Mr Holland—I did not mean to imply that. It is my understanding, which may be wrong, that in the drafting of the bill initially it was discovered later on that the minister was not covered, and that word 'person' was inserted to cover the minister. That is my understanding, which may be wrong, and I will clarify it.

Mr LEO McLEAY—If a person is someone who is an Australian citizen, or even a non-Australian citizen in Australia, who is operationally assisting ASIS, then I have a real problem with this. I do not mind you, Mr Holland, giving them advice, or someone else giving advice or helping to plan, but if someone is out in the field—

Mr Taylor—It would have to be an agent.

Mr LEO McLEAY—Well, with the drafting of this they can be; that is the point.

Mr Taylor—It depends on the definition of 'person', and I think we need to have another look at that.

Senator ROBERT RAY—We have had a look at the explanatory memorandum and that does not help us at all.

Mr Taylor—No, it does not.

CHAIR—Would you get that cleared up and get back to us?

Mr Holland—Certainly.

Senator ROBERT RAY—Am I right in saying that 'publication of identity' on page 25 will substitute for D-notice No. 4?

Mr Taylor—From the ASIS perspective that protects the names and the identities of ASIS officers, and the information that they and former officers obtained whilst they were in ASIS.

Senator ROBERT RAY—That does two things?

Mr Taylor—That does two things. In terms of the D-notice, as I understand it that is a policy issue broader than this. As far as ASIS is concerned this meets ASIS points, but the D-notice question in relation to what happens to D4, the fourth D-notice, is a policy issue which is beyond ASIS's bounds, but it is being looked at.

Senator ROBERT RAY—I understand that, but the point I am making is that there is nothing else in D-notice 4 that is not covered here.

Mr Taylor—I am not sure about that. I do not know the answer.

Senator ROBERT RAY—It is fairly clear about it. What this basically means is that if a journalist—other than referring to you by name, which is allowed—refers to an agent by name in an article or by the ABC in *Four Corners* or something like that, they could be liable for one year's imprisonment.

Mr Taylor—The ASIS officer who passes the name on can and, I think, it applies to the publication of the name only but not to the information.

Senator ROBERT RAY—Yes, but, if next Monday night *Four Corners* runs the names of five ASIS officers, then the reporter who does it and the executive producers and so on can be prosecuted?

Mr Holland—That is correct, Senator.

Mr Taylor—It is in the ASIO Act, as well.

Mr LEO McLEAY—Only if the Attorney-General gives his approval.

Senator ROBERT RAY—As my colleague has just reminded me—I had picked it up, but it is a good point that he is making—why can proceedings only be instituted by the Attorney-General, who is the number one law officer in the land but also a political person?

Mr LEO McLEAY—And who will not want to offend the press.

Mr Holland—Again, I think it was to mirror the provision in the ASIO Act.

Senator ROBERT RAY—I take it, Mr Chairman, that this is because the press have been so mean-spirited in ignoring D-notices out of 'scoop arrogance'. They now can face a year's jail. Prior to that, it was only moral sanction.

Mr LEO McLEAY—That is progress.

Senator ROBERT RAY—Progress has been made.

Mr LEO McLEAY—When are we going to get the answer to the question about the definition of a 'person'?

Mr Holland—As soon as possible.

Mr LEO McLEAY—What does that mean, Mr Holland? I am not a lawyer.

Senator ROBERT RAY—Departmentally, that can mean six months, so we want more a precise answer.

Mr LEO McLEAY—Will I be alive when it arrives?

Senator ROBERT RAY—Hopefully not.

Mr Holland—Yes, you will. We will work on it this afternoon and get it back to you as quickly as we possibly can.

Mr LEO McLEAY—Bearing in mind that this committee has a reporting date.

Mr Holland—Yes, we are aware of that.

CHAIR—I thank both of you very much indeed for appearing before the committee today and for the assistance that you have given.

[11.43 a.m.]

O'GORMAN, Mr Terence Patrick, President, Australian Council of Civil Liberties

Mr MELHAM—Is there anything you want to comment on, Mr O'Gorman, in terms of the evidence that you have heard since you gave evidence?

Mr O'Gorman—I think only on one issue, and that relates to the passing on of criminal intelligence gathered by ASIS. Perhaps I could put in a short written submission to reach you by Friday. Mr Taylor says that ASIS might gather criminal intelligence overseas coincidentally and that ASIS would carry out some activities in Australia via ASIO and use their warrant procedures. My concern remains that via both of those mechanisms criminal intelligence could be passed on to law enforcement agencies. Mr Taylor said—or it might have been Mr Richardson—that that is done now by ASIO as a matter of course. It used to be channelled through the A-G. My view is that there has to be some role for AGIS where, if ASIS or ASIO pass on criminal intelligence to law enforcement agencies, they have to tell AGIS, and somehow or other—I have not quite thought it through in order to address Senator Ray's concerns—AGIS has to be in a position to tell the prosecution that that information exists so the prosecution can fulfil their duty of disclosure.

Senator ROBERT RAY—You are including DSD in that too?

Mr O'Gorman—Yes, I am including DSD.

Mr LEO McLEAY—Can I take you back to the question I asked DSD? I should have asked the ASIS people that question; I am sorry I did not. I asked DSD if they had a problem with a protocol between them and the AFP where it had to be included in the AFP's brief of evidence that some initial steer on this matter came from DSD. They made the point—and I think ASIS made the same point—that a very small part of their product would be material that is passed on to law enforcement agencies. Rather than overwhelm the intelligence agencies with a myriad of requests, would it not be better to approach it from the other end? If the AFP do have some input from intelligence agencies, maybe they just have to put that as a footnote in their brief of evidence—which might allow defence lawyers to then backtrack. Is that a way of doing this that would resolve your worries?

Mr O'Gorman—No, because I do not think you can rely on law enforcement agencies to fulfil their duty of disclosure. I think that is where I have to have a role.

Mr LEO McLEAY—Is that something that you have experienced over time?

Mr O'Gorman—Absolutely. Law enforcement agencies cannot be relied upon to fulfil their duty of disclosure—and that is not just my view. Some do, some do not. But it should not be left to 'some do, some do not'. My view is that, if ASIS or ASIO pass on criminal intelligence to a law enforcement agency, they should tell AGIS. Somehow or other I have got to think of a mechanism that does not become resource onerous for AGIS, whereby AGIS then has the duty to make that known to the prosecution agency when a prosecution is instituted—because the prosecution agency can be more relied upon. We still have problems with them, but they can be

relied upon more than the police to fulfil the duty of disclosure. That is the only point I wish to make.

CHAIR—And you will get back to us on that other matter?

Mr O'Gorman—Yes, I will put something in writing by Friday.

CHAIR—Thank you.

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

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

Committee adjourned at 11.48 a.m.