COMMONWEALTH OF AUSTRALIA

Official Committee Hansard

JOINT COMMITTEE OF PUBLIC ACCOUNTS AND AUDIT

Reference: Management and integrity of electronic information in the Commonwealth

MONDAY, 31 MARCH 2003

CANBERRA

BY AUTHORITY OF THE PARLIAMENT

INTERNET

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

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

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

JOINT COMMITTEE OF PUBLIC ACCOUNTS AND AUDIT

Monday, 31 March 2003

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

Senators and members in attendance: Senator Lundy and Mr Charles and Ms Plibersek

Terms of reference for the inquiry:

To inquire into and report on:

The potential risks concerning the management and integrity of the Commonwealth's electronic information.

The Commonwealth collects, processes and stores a large amount of private and confidential data about Australians. This information is held by various Commonwealth agencies and private bodies acting on behalf of the Commonwealth. For example, the Australian Taxation Office keeps taxpayer records, the Australian Electoral Commission keeps electoral roll information and Centrelink keeps social security, family and health information. The Committee is concerned that the Commonwealth's electronic information is kept securely and in a manner that ensures its accuracy.

In conducting its inquiry the Committee will consider:

- the privacy, confidentiality and integrity of the Commonwealth's electronic data;
- the management and security of electronic information transmitted by Commonwealth agencies;
- the management and security of the Commonwealth's electronic information stored on centralised computer architecture and in distributed networks; and
- the adequacy of the current legislative and guidance framework.

WITNESSES

Committee met at 10.07 a.m.

CHAIRMAN—The Joint Committee of Public Accounts and Audit will now begin taking evidence, as provided for in the Public Accounts and Audit Committee Act 1951, for its inquiry into the management and integrity of electronic information in the Commonwealth. I welcome everyone here this morning to the committee's first public hearing for this inquiry. The committee will seek to satisfy itself and the parliament that electronic data held by the Commonwealth is both safe and secure. The committee will also examine how that standard can be maintained, not just for the present but into the future. It is of key importance to the Commonwealth that its electronic information continues to be assessable in the long term. During its inquiry the committee will take particular interest in the protection of the privacy of individuals and the integrity of information, especially during the transfer of electronic data between agencies or into storage. The safety of such electronic data from unauthorised access will be a major focus of the inquiry.

Today we will hear evidence from a number of Commonwealth departments, each of which is responsible for the collection and safekeeping of a large volume of electronic information. Tomorrow the committee will conduct a public hearing in Canberra, and on Wednesday it will go to Sydney for another public hearing. Further hearings will be held in Canberra in May during the budget session of parliament.

[10.08 a.m.]

McFARLANE, Mr Michael, Auditor, Australian National Audit Office

MEERT, Mr John, Group Executive Director, Australian National Audit Office

NICOLL, Dr Paul, Group Executive Director, Australian National Audit Office

TANKIANG, Ms Jan, Auditor, Australian National Audit Office

CHAIRMAN—Welcome. Mr Meert, do you have an additional statement you would like to make before we start asking you our usual penetrating questions?

Mr Meert—I do not think so. You have got the submission. We have got some additional material which the committee might like to have a look at. It is just a summary of our previous report coverage, which may be useful. We have got it here.

CHAIRMAN—Thank you very much for that. Speaking of your previous reports, can you tell me in general—and perhaps specifically if there were any real negatives—how the agencies responded to your reports and recommendations?

Mr Meert—The general response to our reports and recommendations has been pretty good, although I suppose as a general comment the IT and communication field is a growing field in the public sector, so most public service agencies are still learning how to deal with information capture, storage and retrieval in the new world. There are still quite a lot of them doing a lot of activities towards maintaining that security, but there is still a way to go—as I think our reports will show.

CHAIRMAN—Looking at the key issues that you address and that we are addressing in this inquiry, I am interested that you indicated limited use of FedLink, which is the secure encrypted interagency communications service. Can you tell us a bit about FedLink and tell us your view as to why agencies have been slow on the uptake?

Dr Nicoll—I would be happy to try and answer that question. In 1997, the Prime Minister made his Investing for Growth policy statement. In the statement six years ago, he indicated that he anticipated that the government would move towards a secure intergovernmental Intranet and, following that, the FedLink system was developed. It is an important system which offers a fine opportunity for secure communication between government agencies. There have been a number of enhancements or further launches since then, however the take-up rate is not as high as was anticipated. In December 2002, we had a look at the number of agencies that were using FedLink, and we have included the data on page 16 of our submission. The connection status in December last year was that 14 Commonwealth agencies were connected—five of these were departments and nine were other entities. In contrast, there are 77 agencies subject to the FMA Act and 113 bodies subject to the CAC Act. There is still probably a fair way to go before the potential of this excellent idea and innovation is realised.

CHAIRMAN—But why are they so slow?

Dr Nicoll—We have not done an audit of that, but it would be a question that NOIE might be very interested in addressing because NOIE is the sponsoring agency for FedLink.

CHAIRMAN—Okay, we will have to ask them then. The 2000-01 joint financial statement audits concluded that overall agency management of systems was satisfactory and the systems reviewed had adequate system security in place and their business continuity frameworks assured continuous service. But, in one agency, the financial management system controls could not be fully realised on due to the excessive access to the system and the inadequate maintenance of the account master data and sensitive transaction codes and inadequate change control governing system to system. In another agency there were issues of irregular monitoring by management of security software access. That does not give me a sense of security.

Dr Nicoll—What you are referring to are the results of the set of three IT audits we did in three agencies, and we finished them in that particular year. What we were exploring was whether or not the systems were delivering as specified. One of the dimensions that we touched on was security. There was a range of results. For instance, in one agency, the plans and implementation of IT security was very good but, as you have mentioned, in a couple there were a few problems. But when we identified those problems the agencies responded quite appropriately and quite well, and they sought to take appropriate action.

CHAIRMAN—They did not resent your intervention?

Dr Nicoll—No, they did not. Our experience from all parts of our office is that, when we do work in the area of IT security and find problems, agencies are probably in some ways pleased that we, and not some hacker or somebody else, found the difficulties. They generally cooperate very well.

CHAIRMAN—Out of curiosity, does that include Defence?

Dr Nicoll—In general, yes, I would say that does includes Defence.

Ms PLIBERSEK—I have a follow-on question. You said that they are probably grateful that you are not a hacker. We heard from the Defence Signals Directorate about some security testing that organisations had done that involved paying private companies to try to break into their systems. In one case, the organisation was being tested and they were asked to send off information on a request that was supposedly from the Australian Bureau of Statistics. They found that the organisation responded properly and did not automatically send off the information. Of course, the danger of that sort of security testing is that organisations can inadvertently send off confidential information and they may give away information that comes from other government departments improperly as well.

Can you give us any examples of this sort of security testing where departments have hired outside contractors to do it and contractors have hacked into the systems and found weaknesses or departments have sent off information that they should not have sent off? Can you give us examples of that sort of thing and how you think it is best that departments do that sort of self-testing?

Dr Nicoll—I am not aware of any particular examples. I can give you an example of how agencies can test quite safely, and I think that might be the thrust of your question. In September 2001, we tabled the reports of a 10-agency cross-portfolio review of Internet security. That particular audit actually engaged in some of the kind of testing to which you are referring. The purpose of that audit was to determine the adequacy of agencies' approaches to Internet security.

We did that in two parts. Firstly, we looked at their management framework, and whether they had appropriate policies and procedures with regard to securing their use of the Internet. We also invited the Defence Signals Directorate to work closely with us, and we had their full cooperation. I think it was a really first-class team. What we said to agencies is, 'It's fine to have appropriate Internet security policies, but do they work?' DSD has the capacity to do the kinds of testing to determine whether they were working or not. DSD worked very cooperatively with agencies; they knew what we were doing. If DSD found a hole or a possible breach, it would alert the agency. So it would get up to a hole without necessarily penetrating it. In each of the agencies where we applied this approach, the management and staff were very grateful. I think that would be a fair statement. We also found overall that, in six of the 10 agencies, there were significant vulnerabilities.

Ms PLIBERSEK—Do you think there is enough of that sort of testing and should DSD be the predominant organisation to do it, or do you think the private contractors that are out there do an okay job?

Dr Nicoll—I cannot speak about private contractors, but I do know that DSD did a first-rate, professional job. It would be up to each CEO working within, say, the FMA or the CAC Act and taking account of the protective security manual and different guidelines put out, for instance, by DSD and by NOIE to make a decision like that.

Ms PLIBERSEK—Do you think enough of that testing goes on?

Dr Nicoll—One of the things that particular exercise highlighted was the issue of the adequacy of management monitoring of, in this case, Internet security, which is only one component of the terms of reference. In general, agencies had sound policies and procedures for Internet security; however, we went away and found very significant vulnerabilities in six of the 10 sites, yet in each of those agencies management had done some testing. So I think the question for management is: how much testing is enough? You can never have absolute security; it has to be a risk management approach. Some of the agencies in which there were problems were very important ones indeed, and they had gone about things very well but, notwithstanding that, there were still issues there. I guess it comes back to the notion of risk management and controls in a situation like this—and it is really only management that can make that call.

Mr Meert—The interesting point with that is that I think there are some lessons we can learn from the private sector. I think it would be useful, for example, to have a look at how the banking industry works. They have to test their systems for accuracy, otherwise it costs them a lot of money. I personally think there is room to have a look at how much testing we do. It is very difficult when you have a large system providing continual customer service and you cannot take it down to do testing. There is always a risk that, if you do go and test it, you would take it down yourself. So the real challenge in the public sector is: how do you test it? Do you get somebody to come in and break it? Contracting that out itself brings in all sorts of risks

about contract management. It is one of the challenges in this environment. When you contract it out to IT specialists, how do you control them?

CHAIRMAN—When you said 'we did that testing', did the 'we' mean the ANAO or the Defence Signals Directorate?

Dr Nicoll—Defence Signals Directorate did the actual testing on our behalf. It would have been quite an unusual situation because we would go along and knock on the doors of agencies and say, 'Knock, knock', and they would respond, 'Who's there?', and we would say, 'The Audit Office and the Department of Defence. We are here to help.' It worked very well. We were most grateful for the cooperation of our DSD colleagues.

CHAIRMAN—DSD did the work?

Dr Nicoll—Yes.

Mr Meert—The big question using them is always: are your standards too high? That is an ongoing debate; that is an interesting one to pursue. Are DSD's requirements too high for my business because it costs money?

CHAIRMAN—How does DSD rank in the world in terms of the kinds of operations that they do?

Dr Nicoll—I would certainly say that they have a unique position in Australia, where they quite deservedly have a very high reputation. They are certainly well trusted by government, and I would say with good reason, which is why we decided to work with them.

CHAIRMAN—But you do not know how they rank worldwide?

Dr Nicoll—No.

Senator LUNDY—Going back to the IT outsourcing and reporting to the three agencies that you mentioned, you state in your findings that there were security issues. I did not see that particular report mentioned in the document.

Dr Nicoll—It was a series of reports. We looked at IT in Health, in HIC and in DVA. Each of the results was in a separate report.

Senator LUNDY—Also, the performance audit into the first three IT outsourcing group contracts—cluster 3, group 5 and tax—contained some findings in relation to security, did it not?

Dr Nicoll—The audit was more on the tendering arrangements in regard to that.

Senator LUNDY—That issue goes to the heart of my question. With your observations, those security issues are effectively outsourced, along with the IT hardware, software, networking and services. Can you give the committee an insight into that process of outsourcing or contracting out of all of those things and what effect that has had on security?

Dr Nicoll—Yes, I would be pleased to. In our Internet security report, we found that agencies that had not contracted out—this was a finding that was coming through very clearly—had better communication within the different components of the entity. We actually say that in the audit report.

Senator LUNDY—I think I have quoted it more than once.

Dr Nicoll—Also, when we had a look at the contracts between agencies and their providers, some of them were better than others in terms of providing access to the management of the agency which had the contract and also for the Auditor-General. They certainly varied quite widely in regard to the access provisions for the agencies to see how well the security was being provided on the contractors' side.

Senator LUNDY—I have just asked for a copy to be brought up. From that quite significant IT outsourcing audit that you did of the first three grouped IT outsourcing contracts, my memory says that one of the difficulties was in the prescriptive nature of those contracts, given that they were effectively negotiated by a third party—at the time, OASITO or OGIT in DOFA—and that security arrangements were not effectively prescribed in those contracts, and that led to a whole series of issues that you subsequently identified. Can you confirm if that is the case and recall what your findings and observations were?

Dr Nicoll—With regard to those, I would prefer if we could take a couple of questions on notice. It is a pretty tricky area and I would like to be as sure as I can before responding.

Senator LUNDY—Yes. I am sorry I do not have the report here to quote from.

Mr Meert—I think that what you are alluding to is the complexity when you contract out, especially the further down the track the contracting goes.

Senator LUNDY—That is right.

Mr Meert—We would always see it as a risk. In the end, the agency has to be aware of its own risks in transacting business electronically. You cannot contract that out. You can contract out the technical work to be done, but in the end you still have to make a decision.

Senator LUNDY—You cannot contract out the responsibility.

Dr Nicoll—That is correct.

Mr Meert—You still have to look at it within your own business framework. You can get technical assistance in to look at your operation, but you have to decide, for example, what level of breach you can bear. In some areas, like child support, for example, the risk of having a breach may not be material in dollar terms but it may be quite significant in personal terms for the person whose details have been made public.

Senator LUNDY—Perhaps I will leave the questions on notice and you can come back to the committee with your observations about the risks inherent in contracting out—but also the layers of subcontracting that inevitably occur with the IT outsourcing contracts. In particular,

could we have your observations about the clustered contracts, given that many of those contracts were effectively negotiated by a third party and therefore the agency or department was deprived of managing the strategic approach to security, amongst other things. Further, there is the group management process, whereby these contracts are still managed by a committee of the agencies involved in the cluster and therefore—and I guess I am expressing a view here—their strategic control of their security is somewhat diminished in conveying that to the contractor that is engaged for that purpose. I do not know if there is a question in there somewhere, but I think you know what we are looking for: your observations about how that has impacted. It may just be references to work you have already done but also using your experience as to how that could potentially undermine a stricter security regime.

Mr Meert—In some of our audits—and it might have been the audit of DIMIA—we have identified weaknesses in subcontracting where the contractor has subcontracted without the agency's knowledge. From memory, the recommendation we made was a fairly obvious one that the agency should know who is going to work on these projects. I do not know if there is an answer to what you are saying but, yes, the further you subcontract out, the higher the risks involved in being able to control the process. If you are going to contract out something like IT, you really need to be able to control the lot. You need to know who is going to work on it, because, if nothing else, if somebody has access to the data on the IT system and they happen to be a subcontractor, you need to be aware, for example, of any conflict of interest. You might have a firm that is also transacting some business for somebody else and is in conflict. So you really have to control the process; you cannot subordinate that out to a prime contractor and then say, 'You do this and we will leave it to you entirely.'

Ms PLIBERSEK—I remember a case where people had been accused of selling information that they had got from the Roads and Traffic Authority database in New South Wales. You would not think that that was sensitive information, but it is sensitive if you are someone escaping domestic violence and your address is bought by your ex-partner. You cannot make assumptions about the value of information.

Mr Meert—No. My big point on IT would be that the risk is there whether you transact it on IT or not. Agencies should be aware of the risk of information becoming public that should not be public. We have had cases in the ACT where documents have ended up on the tip. So the risk is inherent. When you start transacting business in different ways, you have to apply that methodology to what you are doing.

CHAIRMAN—Is the private sector inherently more risk prone than the public sector; is that what you are saying? Were you saying that, because someone has an employment contract with the Commonwealth, they can be depended on more than someone who has an employment contract with IBM?

Mr Meert—I would always be loath to compare the public and private sectors. My only point on that is that there is some material that the Commonwealth, by nature, retains which can influence the lives of certain disadvantaged people.

CHAIRMAN—Wouldn't the banks have the same sort of problem?

Mr Meert—Some people in that group—and I am probably getting off the track—may not even have a bank account. They may only transact business.

CHAIRMAN—But wouldn't the banks face the same sorts of problems, and you are not telling me the banks do not subcontract or sub-subcontract?

Mr Meert—That is why I said that I think there is room in the public sector to look at how the banks handle some of their security issues, because they do face the same sorts of problems.

Senator LUNDY—The chair has anticipated where my questions were going: the distinction between security issues and data protection, which is the protection of the privacy of the information on citizens. There is a whole list of examples where data protection has failed and where information has been made public. One example was DEWRSB and the ABN file that was sold by the Commonwealth in CD form—that was subsequently stopped. Can you tell me where the Audit Office is at or if you have had reports on that issue of data protection and how it relates to how you approach security? Can you also tell me whether or not you are seeing an improvement in the understanding within agencies and departments about data protection per se and the inherent risks that come by virtue of things being in electronic form; for example, the difference between a hard copy wad of details and a CD ROM with its ease of access to information and so forth?

Dr Nicoll—One audit we have done in this area was of privacy in Centrelink. We found that, overall, the privacy policies were pretty sound, but the performance information that Centrelink had in relation to the implementation of those policies was incomplete—there was some material but it was incomplete. In regard to that, privacy being a complicated question, Centrelink staff apply a proof of identity test to determine that that person is that person. Those proof of identity tests are essential for ensuring that the data are accurate, the data have integrity, the data are of the right quality and, thus, payments are controlled. Our office did a retest of the sample and there was a 22 per cent error rate in regard to the application of the proof of identity test. We are not saying that 22 per cent of payments were wrong; we are saying that the probability of erroneous payments certainly increases when you have problems with the integrity of data.

Ms PLIBERSEK—When you say that 22 per cent had errors, could that mean 'Mrs' instead of 'Mr' in the address line and things like that? Are you talking about a very broad range of errors?

Dr Nicoll—It is a broad range of errors, yes, but overall in those cases Centrelink's own proof of identity tests were not correctly applied.

Ms PLIBERSEK—That might be partly accounted for by the fact that if you were a homeless person, for example, the likelihood of your having accurate documentary evidence of who you are would not be high.

Dr Nicoll—In those cases it is very hard for Centrelink staff—let alone for the homeless person, obviously.

Ms PLIBERSEK—Or someone with a mental illness, for example.

Dr Nicoll—That is correct.

Senator LUNDY—In the audit supplied as part of the submission, could you include the original IT outsourcing?

Dr Nicoll—Yes, we will certainly do that.

Senator LUNDY—Could you also include the audit into the health cluster tender? That too contained issues relating to security. In particular, on the issue of data protection, it is now well known that final pricing information was conveyed in an electronic format to competitors, and the issue was well-canvassed in that audit. Both of those reports are extremely pertinent to this inquiry.

Dr Nicoll—Okay.

CHAIRMAN—One of the things that concerns me is the issue of data transfer between departments. We talked to the Child Support Agency—and you mentioned CSA, Mr Meert, a minute ago—on Friday. I cannot recall what CSA said about that and my advice is a little bit slow. I am sure that Ms Plibersek is right in saying that there is a two-way exchange of information between CSA and Centrelink. I know that Centrelink exchanges information with Tax, Health and no doubt other agencies. What I am not sure of is whether CSA information also goes to those agencies or whether it only goes to Centrelink. Surely the complexity of line items and the number of information sources included in the transfer makes that labyrinth more subject to failure somewhere along the line. Have you done any work towards testing that integrity?

Mr Meert—No, we have not tested the integrity of the data in that sort of transfer.

CHAIRMAN—I am sure of what their answer would be if I asked them.

Dr Nicoll—Mr Meert is quite correct. However, we have touched on this area of electronic exchange of information in a few other audits—for instance, in the audit we tabled last year on the implementation of the 30 per cent private health insurance rebate. It is very important that HIC and ATO agree on the data. They did have some difficulty in getting a successful reconciliation of their data electronically, and we drew attention to that in the report. They have taken great strides since then, but it took both of them quite a while to make sure that the data they had on the same individuals from the same funds was reasonably consistent.

CHAIRMAN—Was that a failure with Medicare card numbers?

Dr Nicoll—No, it had nothing to do with the failure of the Medicare card numbers; it was due to the fact that HIC and ATO were getting slightly different information from the private health insurance funds. They have now been made aware of this and are working very hard to take giant steps forward to address this difficulty.

CHAIRMAN—But you have not done any work to determine whether, in transferring that data, it becomes susceptible to hacking or release to the outside environment?

Dr Nicoll—No, not in regard to that particular one.

Ms PLIBERSEK—Regarding the example that the chairman is talking about, with departments exchanging information—Centrelink with Tax, the Child Support Agency with Tax and Centrelink—my electorate office has been told of instances where Centrelink has exchanged information with corrective services or the parole office in New South Wales and it has become apparent that they have stuffed up. It was very serious—the wrong person had their benefit cut off. They walked into the Centrelink office to ask why and were told that they should be in jail and not in receipt of benefits. The root cause of that was identity theft, which is something else that the DSD raised when they came to see us. They talked about the ease of creating another identity, particularly to obtain benefits or, I suppose, to avoid some other liability. Have many examples come up in the course of your audit where this has been an issue that you have examined?

Dr Nicoll—I did not come across any examples quite like that, but I will draw your attention to two other items which might be relevant. In October last year, the Management Advisory Committee released a very significant report. It was called *Australian government use of information and communications technology: a new governance and investment framework*. The Management Advisory Committee reported that there was no whole of government approach to the authentication of individuals who must undertake different processes with different agencies when identifying themselves to access government services. The Management Advisory Committee also concluded that business authentication is significantly more developed than individual authentication. There is some awareness of this, but there is also some awareness of the difficulty in addressing this particular issue holistically.

Ms PLIBERSEK—Are we back to the Australia Card then?

Dr Nicoll—That is a policy question; it is not for us to answer.

Mr Meert—But there are other ways. The Health Insurance Commission has some interesting IT systems which track people's movements around Australia to see if they are duplicating on doctors. So there is some stuff around in the Commonwealth.

Ms PLIBERSEK—How do they do that? Are you talking about people who use their real names? How do you do it if a person has more than one identity?

Mr Meert—The identity thing is interesting. Even if Centrelink got somebody and transacted it physically, the identity fraud is a problem whether you use it electronically or not. The opportunity electronically is that people can use other means of creating a false identity. The problem is the same but the opportunities have grown. What we say as an audit office to a place like Centrelink is: you really have to determine how this electronic commerce is helping people to develop new identities, because they could do it before.

Ms PLIBERSEK—What about the flip side of the argument? This sort of free exchange of information between departments quite seriously disadvantaged the constituent that I am talking about. Not only did she lose her benefits for a number of weeks, but she was humiliated when she went into her Centrelink office and was told that she should be in jail. Does the lack of appropriate protocols in a situation like that have possible consequences?

Mr Meert—There are probably some more significant problems there than the electronic means of transacting that piece of business—

Ms PLIBERSEK—Except that people believe it—if they have got it off the computer, they do not question it as much as—

Mr Meert—True, but the request could have come through on a fax machine. People believe faxes as well. My point is that you now have this opportunity to electronically transact business very quickly. Perhaps you have to consider slowing that down to make sure you do the appropriate checks. We have all sent emails and then regretted them. Sometimes the speed of the business is so quick you have lost sight of the risks of doing that.

Senator LUNDY—In relation to the Protective Security Manual that agencies are supposed to comply with, have you ever done a full audit of all agencies and departments and their relative compliance with that document?

Dr Nicoll—I do not believe that we have. We have looked at certain aspects of it with some of our assurance audits, but not holus-bolus in its entirety. However, the Internet security report, which I mentioned earlier, did take account of the Protective Security Manual and sought, for instance, to determine whether agencies had integrated its requirements into their internal policies.

Senator LUNDY—What is the status of the Protective Security Manual for agencies and departments?

Dr Nicoll—I understand that it is a document put out by the Attorney-General's Department, and it contains a set of requirements and sound advice. It is a combination for agencies to follow to ensure that their physical and other assets are as well protected as possible, and obviously electronic data are included under that.

Senator LUNDY—There is another standard that sits beneath that—ACSI 33—that relates to electronic data.

Dr Nicoll—Yes.

Senator LUNDY—Is that mandatory?

Dr Nicoll—It is certainly highly advisable. I think it is mandatory. My colleague Mr McFarlane might be able to answer that.

Mr McFarlane—The PSM actually defers to ACSI 33 and to DSD as the Commonwealth computer authority. In that sense it is mandatory, because PSM calls it up and says, 'When you are dealing with electronic information, refer to this.' As I recall, the PSM has a number of mandatory and non-mandatory, or advisory, components.

Senator LUNDY—Has the Audit Office ever audited adherence to ACSI 33 in part or in full across all agencies and departments?

Mr Meert—No, not across all agencies.

Dr Nicoll—Something like that would be a very big undertaking.

Senator LUNDY—Yes, it would. Are you able to point to any exercise by agencies or departments themselves—perhaps their own internal audit or quality control measures—that could give the committee some clue as to how the departments are faring in their compliance with that particular regulation?

Dr Nicoll—The audit which comes to mind is the one I mentioned previously in terms of Internet security. We found a range of responses there from particular agencies. Different agencies consider them at different levels. The department of health was pretty good in terms of its taking account of requirements like that. I mention that because it is one of the three agencies that we did these particular IT audits on a year or so ago.

Senator LUNDY—You mentioned a report on, I think, a new governance and investment framework from the management advisory authority. Is that the same document that was produced by Prime Minister and Cabinet?

Dr Nicoll—Yes, it is.

Senator LUNDY—What other security related issues did that paper raise?

Dr Nicoll—It sought to establish a chief information officers committee, and I understand that that has been established. It has referred the issue of the facilitation of a Commonwealth agency work plan for information and e-security to the e-security working group. NOIE coordinates that particular working group, and I know it has certainly had a couple of meetings and is proceeding forthwith.

Senator LUNDY—When was that report published?

Dr Nicoll—It was published in October 2002.

CHAIRMAN—Thank you very much for your submissions, your audits and your attendance today.

[10.54 a.m.]

MEE, Mr Tony, Assistant Secretary, Business Information Solutions Branch, Department of Family and Community Services

CHAIRMAN—Welcome. We have your submission, which we have published. Do you have anything you would like to add to that submission?

Mr Mee—No.

CHAIRMAN—Your submission says:

FaCS holds the view that the Commonwealth in general needs to pay greater attention to the preservation and access of data holdings over time. There is no whole of government strategy or resources for identifying data sources across agencies that need to be preserved over long periods of time. There is also a need to ensure that such data remains accessible over changes of technology including software.

CHAIRMAN—Can you expand on that for us please?

Mr Mee—Yes. As government agencies move increasingly towards capturing and retaining information in an electronic format, the volume and the size of that data and the importance of that data will continue to grow and really there is no clear broad-based framework for protecting that data over a greater period. You need to ask: will that information be important in 20 years time? How will we manage it? How will we retain it? How will we classify that information over those sorts of time frames?

CHAIRMAN—Are you identifying only how we retain it over time or are you also identifying that there may be a security problem the longer out you get?

Mr Mee—Retaining that information is more the issue rather than the security side of it. I think the sorts of security controls that agencies put in place will continue through the life of that data, but it is actually being able to continue to access that data and being able to attach meaning and value to it.

CHAIRMAN—There is quite a lot of data transfer between agencies.

Mr Mee—Yes.

CHAIRMAN—And I would think your department is right in the middle of a lot of it.

Mr Mee—The focus of the core FaCS department in terms of information and the sort of information that is exchanged is primarily for policy analysis and advice. We do make that available to other agencies. We do get information from other agencies and we do access Centrelink information, in particular, for the purposes of doing that sort of policy analysis.

CHAIRMAN—But you are responsible for Centrelink, aren't you?

Mr Mee—Yes, essentially.

CHAIRMAN—And Centrelink is the very heart and core of a great deal of data transfer.

Mr Mee—Yes.

CHAIRMAN—Does FaCS do work internally—or do they have an external audit or test done—towards satisfying itself of the security of data transfer between all those various bits and pieces and Centrelink and back again?

Mr Mee—Generally there is a set of explicit frameworks governing those data transfers and the management of that data. In terms of reassurances, there is a range of audits done—and I do not know the specific details of those—which, from a FaCS perspective, would be done with a view to ensuring the security of that information. Centrelink itself undertakes a whole lot of work in that space. Generally, I think the approach would be that Centrelink would undertake that work and make the results of that work available to us.

CHAIRMAN—We understand that Gatekeeper is the Commonwealth government's strategy for the use of public key infrastructure, delivery of online and e-commerce. According to the National Office for the Information Economy, FaCS has not applied for Gatekeeper accreditation. Can you tell me why?

Mr Mee—FaCS itself really does not have many systems at this stage that could really profitably make use of PKI infrastructure. That is basically the reason why. We do very little transacting electronically in terms of web sites and so on where we need that sort of framework.

CHAIRMAN—You are, however, connected to FedLink.

Mr Mee—Yes, we are.

CHAIRMAN—How well does that work in your view?

Mr Mee—At this stage, we have a physical connection to FedLink, but we will not actually start using it until about May. The intention is to use it for secure email between government agencies.

Senator LUNDY—How long have you been participating in FedLink?

Mr Mee—We connected to it last year—I am not sure of the date—with the intention of being able to exchange secure emails. This will be a better way of working with a number of government agencies than currently. Beyond the physical connection, we have to make changes to our internal mail system to take advantage of it. That work is currently being done to get us across there. Our view is that, once we are on, a whole range of information will get exchanged with other agencies. Currently there is a variety of ways of making it work because of the security concerns. Doing that, will give us a much more flexible capability.

Senator LUNDY—Given FedLink has been around for a much longer time than that, what led you to that decision last year? Were there issues about the integrity of your systems? What

prompted you to go there, given that it was obviously a big decision if you are still making the software changes necessary to make use of it?

Mr Mee—We have been doing a range of work to improve the security of our network. It was just a staged part of that broader work. In fact, we have referred to some aspects of that in our submission. It is really about where we got to after doing other work; it was time to look at this.

Senator LUNDY—What about redundancies or backups within your systems, particularly the networks? How well are you positioned to respond to any major problem in that communication network with other agencies and departments?

Mr Mee—Centrelink is the exception. We have a secure connection with Centrelink now and we obviously do a lot of electronic communications with them. There really is very little redundancy in terms of the agency connecting electronically to other agencies.

Senator LUNDY—Is that a concern to you?

Mr Mee—No. I think the broader concern is obviously a redundancy around our own network because we run a number of state offices and we have redundant links in that case. The connection with Centrelink is important because we do so much work. As we move to FedLink and we start to use that more heavily, I suspect that will become a stronger focus for us.

Ms PLIBERSEK—The submission from the Federal Privacy Commissioner mentions an incident in June 2002 involving email addresses collected from a FaCS web site. The web site editor sent an unsolicited marketing message to these email addresses on behalf of a third party. Can you tell us about this? Can you tell us what has been done to prevent a recurrence of this sort of privacy breach and tell us more generally about the penalties that apply for breaches of customer confidentiality and what sorts of examples you have had of that recently?

Mr Mee—In relation to the investigation last year by the Privacy Commissioner, the matter was around the collection of email addresses for valid purposes and their reuse for something else.

Senator LUNDY—Can you tell us what the person was marketing and who the third party was?

Mr Mee—It is a youth site. I am not aware of all the details but my understanding is that they collected email addresses in a discussion forum and then used those to market a competition, which was an internal competition of some form—

Senator LUNDY—It was still a FaCS competition; it was not sold to Coca-Cola.

Mr Mee—No. I am not aware of all the details but that is my understanding. There was an investigation flowing on from that. There was obviously an education campaign directed at business owners of web sites in FaCS. There are tighter procedures around how content is used and gets onto web sites. In terms of recurrence or subsequent breaches, I am not aware of any. I do not believe there have been any.

Ms PLIBERSEK—You do not believe there have been any.

Mr Mee—I would know about it and, no, there aren't any.

Ms PLIBERSEK—I find that surprising in an organisation the size of yours, that there aren't occasional breaches. I would have thought that it was almost inevitable in a big organisation.

Mr Mee—In terms of the sort of information and so on that we manage, it is fairly tightly controlled. It is probably worth while saying that much of the information that we hold is held for policy reasons, so it is de-identified information and so on, so we do not have quite the same capacity for breaches as some other organisations have.

CHAIRMAN—Outside of DSD certifying your gateway and firewall environment, do you use them for any other purposes? Do you have any other relationship with DSD?

Mr Mee—Basically we use them for all our external connections, which is fundamentally the web stuff, but also things like dial-up access to a network. All that comes through the DSD approved firewall gateway.

CHAIRMAN—Do you elicit the services of any outside agencies, including DSD, to test your security integrity from time to time, or do you just rely on your systems?

Mr Mee—There are a small number of DSD certified providers of security testing and vetting services. We do engage them from time to time to look at specific areas that we want to test.

CHAIRMAN—Has that resulted in change of department policy?

Mr Mee—In some cases it could result in changes to policy. Largely there have been external hacking or vulnerability type tests that we have done with providers. We have also used them to look at our procedures and to vet parts of our infrastructure and so on to make sure it is compliant.

CHAIRMAN—You said you do not do much data transfer between other agencies. Does that include Centrelink?

Mr Mee—As I said at the beginning, we do access Centrelink systems. In the main that is what we call strip files and so on—large customer files. We run analysis jobs for use in policy research. That is the main activity.

CHAIRMAN—Do you do anything to assure yourselves—and to be able to assure us—that information when transferred from Centrelink to FaCS is not vulnerable to external release?

Mr Mee—In terms of the Centrelink data, we have connections into the Centrelink network, so most of that work and much of the data that we use is stored on Centrelink systems and is subject to all the same controls that Centrelink has around its information. In terms of the portion of the information that we do transfer across to our own system, there is a whole lot of process controls and security wrapped around the management of that. In many cases, and

certainly for the prime data sets that we keep on our network, the information is de-identified. We do things like removing the Centrelink customer's name and changing the Centrelink customer record number to a different number, to reduce the chances of that information being misused.

Senator LUNDY—What interaction do you have with NOIE, who are effectively providing the secretariat services and all sorts of other things to the Chief Information Officers Management Group, and also DSD, given their role in security and encryption matters?

Mr Mee—We are represented on the CIO committee and the IMSC—I think that is the name of the other body. We are also represented on a number of the working groups that NOIE have set up. Those things are gradually working through; it is early days for those working groups. In terms of DSD, we do not have any representation there at all. Our gateway is supplied by 90 East; it is outsourced. It is DSD approved but we have very little direct dealing with DSD.

CHAIRMAN—Thank you very much, Mr Mee. If we have further questions, you will not mind if we put them to you in writing rather than have you come back again?

Mr Mee—That is fine.

[11.15 a.m.]

FEGAN, Mr Patrick, National Manager, Business and Information Protection, Centrelink

TREADWELL, Ms Jane, Deputy Chief Executive Officer, Digital Business and Chief Information Officer, Centrelink

CHAIRMAN—Welcome. Thank you for your submission, which we have received and published. Would you like to make a brief opening statement or shall we start asking questions?

Mr Fegan—Firstly, I would like to provide the committee with an information pack that you might find useful as reference material.

CHAIRMAN—Thank you.

Mr Fegan—Secondly, Centrelink has a very strong privacy culture that permeates the organisation and is backed up through our training, policies, procedures and IT framework. Protecting the information of Australian citizens is essential to our core business and is an asset that we value highly. We take seriously our obligations in that regard and we work very closely with the Privacy Commissioner.

CHAIRMAN—I noted in your submission your description that you have a strong privacy culture. How did you get there?

Mr Fegan—Over many years.

CHAIRMAN—Not that many—you have not been around for very many.

Mr Fegan—That is right. It goes to the heart of the business. A large part of the business Centrelink undertakes—we have a range of other functions, naturally—is, of course, making income security payments to the Australian public. To do that, we need to capture a lot of personal information to enable us to accurately assess a person's entitlement. People will not provide us with information if they do not trust us. I think the committee would also see from the Privacy Commissioner's submission that the general public have a relatively high level of trust in government enterprises. Our own surveys indicate that we have a trusted status.

Training is one of the key elements. If you join Centrelink, we provide you with a good deal of induction training that focuses on your privacy obligations. We get people—including contractors and so on—to sign things. Every time a member of staff logs onto our system there is a splash screen that says, 'If you are going further, be aware of your obligations.' An example of that is in the information pack. At the same time, we investigate thoroughly any breaches or potential or alleged breaches. We take those seriously. We track and log every access made by our staff to the customer database, so there is a full history besides time and date stamps. If there was inappropriate access, there would be no question that Joe Bloggs, for instance, had accessed that particular record and we would have the full history of that.

Ms Treadwell—Privacy legislation in the 1980s began the journey, so we have had the experience of managing customer information in a very regulated way for over 15 years now and the organisational arrangements are in place. There are privacy officers throughout Australia who link back to the national policy group but are also very much involved in the day-to-day operations of each of the areas.

CHAIRMAN—I hear you, but this committee also is aware, because we have further inquired into ANAO audits, that the degree of bureaucratic accuracy surrounding your database is quite suspect.

Mr Fegan—I am not sure that we would concur with that overall assessment.

CHAIRMAN—Certainly the last audit—which was, if I remember correctly, was new people requesting entitlements—

Ms PLIBERSEK—Age pension entitlements is the one you are thinking of, I think.

CHAIRMAN—Okay. It was new people trying to access age pension entitlements, and there was a high rejection rate found by ANAO. How does that give us confidence, if ANAO is not that confident in your database, that your security culture actually works? Does that make sense?

Ms Treadwell—I think I know where your question is coming from. I think it is very important to look at the findings of the age pension audit and the subsequent work that was done to assess that level of finding and the cause for some of the errors. There was a high level of inaccuracy on the part of the customer providing us with information and subsequent changes in the income support payment, as compared with the issue around privacy and security management of customer data.

CHAIRMAN—My memory tells me that there was also a substantial failure rate with regard to data entry; that is, failure to determine a person's nationality or address, not filling in the lines on the electronic form properly, missing data which would be required for security or for confirmation of the client, et cetera. I recall that that was very high.

Ms Treadwell—And my understanding of the JCPAA hearing was that our CEO provided a lot of information about the steps that Centrelink took, and has taken since that audit, to improve our procedures and to find ways for customers to be able to update their circumstances with us so that those payments are made more accurately. We certainly understand that the income support information that drives the payments is very important, and the way in which we manage the customer-staff interface, the skills of our staff in entering and questioning that information, and the system material are also very important. It is all part of an overall system. The data privacy and security management is a component of that.

CHAIRMAN—I have no desire to revisit either that audit or our inquiry but simply to ask: if you cannot get each file 100 per cent to start off with, how can you guarantee that the security and privacy is upheld? If you do not know who I am, how can you guarantee that my privacy is intact?

Ms Treadwell—Our driver is to make our system very strong—our people management systems, our customer relationship arrangements and our IT systems.

CHAIRMAN—In a public hearing with the Child Support Agency last Friday, we were told that there is a two-way exchange of information between Centrelink and the CSA. I am unsure of whether they also indicated that there are a number of other agencies that you receive information from—for instance, the tax office, the health department, the Department of Veterans' Affairs or whatever. That feeds into Centrelink and then the Child Support Agency accesses that information third-hand, if you will. Is that right? Or do they directly access those departments as well?

Ms Treadwell—We may have to get particular information to you on the detail.

CHAIRMAN—Do you understand the generality of what I am asking?

Ms Treadwell—Yes. There are two types of data exchanges that we perform in Centrelink. One is under the very strict provisions of the data matching authority and act, and that picks up the points I think raised earlier in regard to correctional services authorities and the Department of Veterans' Affairs, where there is a requirement for data matching between the tax office and Centrelink and a whole range of other organisations. Those conditions for that data matching are tightly controlled and observed through both the Privacy Commissioner's office and the controls underpinning that legislation, and that occurs on a regular basis—the information is brought together, the data is matched and then that customer data goes back to the originating authorities. So there is that type. Then there is that type for which data is provided under social security legislation. That would be where the children's services agency links with and provides information to Centrelink, where there are adults and children under split family arrangements where income and income support are managed through such a regular exchange.

CHAIRMAN—Let's say there is an agency that feeds information to an agency that feeds information into the tax office which feeds information to you who feed it to CSA. My question really is: doesn't every increase in the length of that chain increase the likelihood of breaches of security? Any risk management analysis tells you that the longer that gets, the less secure the data becomes.

Ms Treadwell—From your perspective I can see that, the longer the chain is, the greater the risks or the more points of vulnerability there are from a high level of abstraction. The point I did not make before is that, where customer data is moved from one organisation to another, it is done with the full knowledge of the customer. That is where people are informed, or should be informed, that it is under legislative provisions or that permission is sought to use it again. Even in Centrelink, where we might already hold data on someone, at times we have been required to ask for permission to use that data again. In the broader elements, in terms of an environment whereby information is exchanged between organisations, as we find in the commercial or customer convenience world, it certainly puts more pressure on those areas that manage these electronic communications to look for risk and to reduce that risk.

CHAIRMAN—In this data transfer environment, do you have many breaches of security? Do you have any failures?

Mr Fegan—Within our current environment our exposure to the outside world is quite limited. Externally, we have a DSD certified gateway. That was certified last year, so we are applying the best technology and practices that we are able to, and there are a number of firewalls within that. Our current network is analogous to a fortress. We have good and effective access controls, so only those who have a right by virtue of the position they occupy can access the data. That data is logged. The links that we have with other organisations are all authorised. There are encrypted links. For instance, within Canberra we use the Icon network, which is dark fibre. We have effective layers of security in place in terms of our various applications and our various IT platforms.

In a general sense, perhaps coming back to the first point too, there are many opportunities where an existing customer has an opportunity to correct and/or update the information they may have provided us through a regular review. If they have changed their address or have telephoned a call centre, we will update some key information. So there are opportunities there if, for instance, there was some incorrect information provided by them and/or misrecorded by us. There are plenty of opportunities over a period of time in terms of our day-to-day dealings with them to correct mistakes, if there are any.

In terms of external penetration of our systems, as has been discussed earlier this morning, we also seek competent advice in terms of the adequacy of our system through a range of external providers. We work and consult with DSD, although I sense that DSD's capacity, if you like, to be the main provider in this game is somewhat limited. In fact, I was in a meeting with them only three weeks ago and I was exploring with them then their capacity, if we were to hire them, to do some specific work for us. They seemed a little bit reluctant. They have a process in place for any of the particular products or arrangements and we consult very closely with them to get their advice and input that we have got adequate risk management plans in place. That is all part of maintaining the continuing accreditation of our gateway.

CHAIRMAN—You did not answer the question. Do you have many breaches?

Mr Fegan—We have no breaches to my knowledge.

CHAIRMAN—And that has been tested by DSD?

Mr Fegan—I think it is a bit like John Meert from ANAO would have identified. We have in place fit for purpose products and applications and a security regime. Our gateway provides lots of levels of protection. We know we get probed through the gateway, but that is all logged and rejected. To my knowledge, we have not had any proven instances.

CHAIRMAN—That is a definitive answer.

Ms PLIBERSEK—First of all, I would like to ask you if you would send us a complete list of the organisations that you do data matching with and a complete list of organisations that you swap information with under the social security legislation that you mentioned.

Ms Treadwell—Certainly.

Ms PLIBERSEK—Ms Treadwell, when you say that information is only exchanged with the full knowledge of the customer, that seems a little strange to me, because Mr Charles and

Senator Lundy would know that we often have people coming to our offices who are perplexed by some action that Centrelink has taken. The example that you may have heard earlier that I recounted was a woman who was cut off benefits because someone had used her name when picked up by the police and had been charged under that name, and may even have been incarcerated under that name. The data matching between Corrective Services and Centrelink led to my constituent being cut off Centrelink benefits. I am sure that my constituent was not approached about allowing data matching between Centrelink and Corrective Services or she would have been alerted to the problem before being cut off benefits. What do you mean about informed consent?

Ms Treadwell—Informed consent for us to use it beyond that which the legislation actually requires us to apply.

Ms PLIBERSEK—Does that mean that when you first sign on to get your unemployment benefit you sign a form then, or does it mean at a subsequent stage? It is not really informed consent if people's options are to receive a benefit or not receive a benefit if they do not fill the form in properly, is it? They have got no right to say no, do they?

Ms Treadwell—I think the Privacy Commissioner has views about this as well, but certainly there is the legislation under which the income support payments are made. People who are seeking income support are required to fill in a claim form. We observe the obligations and the arrangements under which that legislation is administered. The point I was making is that our staff are encouraged and trained to alert all customers of those obligations and the conditions under which those payments are delivered.

Ms PLIBERSEK—To be clear, you have the option of receiving a benefit or not receiving a benefit if you are not prepared to let your information be subject to data matching or other exchanges of information between government departments. They are your options, aren't they?

Ms Treadwell—We administer the legislation.

Ms PLIBERSEK—I hope it does not sound like I am accusing you of anything. I am just clarifying what a person's options might be.

Ms Treadwell—Where we might find an efficiency internally that we can use that information we seek permission to use it.

Ms PLIBERSEK—Can you give me an example of that?

Mr Fegan—For instance, one of the very useful facilities we offer our customers is in relation to a system whereby we will make payments for the rent if they are with a housing authority. They would confirm that they are in public rental housing and authorise us to pay a particular proportion of their payment to the authority.

Ms PLIBERSEK—It is a direct debit.

Mr Fegan—It is like a direct debt. You have full control over that. You can turn it off at any time. That sort of client confirmation is a service that we offer. People find it of advantage.

Ms Treadwell—The information stays with us, which is a check as to whether that person is an existing customer of Centrelink.

Ms PLIBERSEK—Going back to what you said earlier about clients being informed, if their information is being shared with another agency for data matching purposes, are they informed of that?

Ms Treadwell—There are millions of data matching arrangements that occur during the year.

Ms PLIBERSEK—I know that.

Ms Treadwell—It would be more in the course of: this is the way Centrelink performs its duties at the earliest.

Mr Fegan—For instance, family customers would be aware that we would match with the tax office and send it as a confirmation of their declared earnings and things like that. We have communication products that outline this in broad terms.

Ms PLIBERSEK—You have raised families and their relationship with the ATO. That of course is very relevant because of the overpayment that many families have experienced recently that has led them to have family tax benefit debts. How quickly do you inform your customers if some anomalies come up that require their attention? Do you give them the opportunity to explain to you when, for example, data matching throws up some anomaly? Sometimes there is a perfectly reasonable explanation that should not involve someone being cut off benefits and then having to come to you and explain, and there is inevitably a delay of several weeks between the last cheque they get and the next cheque they get. What processes do you have for asking people to explain what you discover?

Mr Fegan—If, for instance, the data matching showed up undeclared earnings and that became evident, we would contact the customer to say, 'Can you please provide an explanation of this?' before we go ahead and raise the debt or—if there were a series of breaches—it leads to some prosecution activity. We see that example many times. For instance, job seekers might put on their net income as opposed to their gross income. They may declare income at the time they earned it as opposed to when they actually received it. All that sometimes leads to problems. That is regular business for us, and we have well-defined processes in place for dealing with that. Customers have an opportunity to provide an explanation to correct any errors of fact and to put some context around it.

Ms Treadwell—The experience that one of your constituents had is not one that we would like to think exists generally, and we would be very keen to follow that up.

Mr Fegan—That was a stolen identity—

Ms PLIBERSEK—I have discussed it with Centrelink, and they very quickly apologised. My view was that the woman had been defamed. She was told, in the middle of a crowded room, that she should be in jail. That is not just a little error. I regard it extremely seriously, and I am happy to say that the higher Centrelink management realised very quickly that they were on very thin ice.

I do not want to keep harping on an individual case, but it just seems to illustrate so much about what this inquiry is about. This person had no idea that her information was being shared with Corrective Services, and she was given no opportunity to correct the public record. She was cut off benefits and then had to defend herself. She had to convince Centrelink that she was who she actually was.

Ms Treadwell—I think Mr Fegan has gone through what we expect the process to be, and we will continue to pursue a much stronger ability for our front counter staff to be able to apply appropriate procedures in a customer service environment and the public environment.

Ms PLIBERSEK—I have two more quick questions. The Australian National Audit Office suggested that perhaps one of the reasons that we hear so many stories like this—and I can assure you that we do hear them as members of parliament—may be because of the speeding up of the transmission of data between organisations. If you can check a thousand records a year, you are not going to have as many anomalies thrown up as you would if you can check 100,000 in a month. Do you believe that, with the speeding up of the transfer of information, appropriate secondary investigations exist? Data-matching melds two sets of figures but does not examine in any detail what the possible causes for the anomalies might be. What sort of secondary checking do you do before you start sending out letters?

Mr Fegan—I guess it would depend on the particular match. For instance, we do match with prison authorities. Our expectation would be that we would not continue payments to customers who have gone to prison. For a start, that avoids a large overpayment, but it would not be practical for us to confirm that each and every one of those individuals is in prison. To some extent we are entitled to rely upon the advice of the competent authority. Where we seek to recover funds from an individual, at all times they have an opportunity to explain how an anomaly has occurred and to seek a review of that particular decision in case there are any errors of fact involved. Then there is a range of levels of appeal thereafter.

Ms Treadwell—The data-matching process has been in place for many years. In regard to the whole arena of electronic commerce or electronic government, there are developments that take advantage of technology but the value of electronic communications is that it is supplementary and complementary to other existing services, from a Centrelink perspective. In the old days when there were clinically separated data-matching procedures, someone in prison, for example, might not see someone from the social security department or Centrelink until two or three weeks after they were released.

Much of the work that Centrelink has been pursuing in the last few years is to try and link our services to those of other organisations—including prisons, correctional services authorities and the non-government sector—in a service support role whereby we may well be dealing with the prisoners and their families even before release. There are some very exciting developments that we are now pursuing where we have Centrelink staff visiting correctional authorities before release in order to make it much easier for prisoners and their families once release occurs. That might be secondary but it is a much more service supporting development and the data-matching work is the fraud control element. As we get a stronger mix and complementary service arrangements in place, I imagine the risk of independent cut-offs will be lower.

Ms PLIBERSEK—In 1999 Centrelink was the subject of an ANAO performance audit of its management of data privacy. That audit found that Centrelink applied aggression tags and that

they were inconsistent with privacy principles. The idea, obviously, is to identify hostile clients. But the audit identified that that could be an infringement of privacy and that tags were not reviewed regularly, and that you might have problems with ongoing accuracy if you were identifying people that way. I understand that Centrelink staff do a very difficult job and that they often have to deal with clients who are hostile and even, occasionally, violent. I would like to know how you balance your responsibility to your staff to provide them with a safe workplace with your responsibility to clients not to have them identified as violent, when perhaps there was an incident 15 years ago that should not really be on their records any more.

Mr Fegan—We have certainly tightened up our processes around that particular indicator.

Ms PLIBERSEK—How do you do it now?

Mr Fegan—It is a necessary indicator. The other element is our obligation to other providers who might have dealings with us. There is no hard and fast rule there. To some extent the best solution is to provide well equipped, well trained staff. The way in which they deal with individuals in difficult circumstances is to avoid the situations in the first place by very effective listening and an understanding of their particular concerns. There are other situations where customers who deal with us from time to time have a lot of other issues in their lives or may have particular mental illnesses, and things like that. Sometimes we would tag an individual and a more experienced customer service officer might choose to deal with them so that they have a better rapport with one or two individuals as opposed to those who front at the counter. Sometimes we might exercise our discretion on the amount of times we would call them in or have them come in and lodge forms, by putting on variable lodgment periods so that there would be less interaction and therefore fewer opportunities.

Ms PLIBERSEK—If someone is on a disability support pension, how often would you normally expect to see them?

Mr Fegan—That is not my particular area.

Ms PLIBERSEK—You do not need to put in a jobseeker diary if you are on a disability support pension.

Mr Fegan—That is right.

Ms PLIBERSEK—You would only be seeing them a few times a year, anyway.

Mr Fegan—You would only be seeing them periodically. That is not my area. I guess I could not answer that.

Ms PLIBERSEK—You still tag people. Do you review those tags?

Mr Fegan—I want to come back to you with the detail of the processes we have in that place.

Senator LUNDY—I would like to go to more general issues but, in particular, Centrelink's involvement in the management advisory committee on IT related matters. Could you tell me how Centrelink is involved and which committees either of you are on within that structure?

Ms Treadwell—The CEO is on the Information Management Strategy Committee, I am on the CIO committee and a number of people from Centrelink are on the various working parties.

Senator LUNDY—That gives me enough to work with. I know I am talking to the right person. Page 14 of the Management Advisory Committee report *Australian government use of information and communication technology: A new governance and investment framework* talks about information reuse. I will just quote from it:

> Subject to appropriate privacy and security treatment, information sharing can improve the efficiency of business processes within government and streamline government service delivery to citizens and businesses. ICT is the key enabler …

It goes on to say:

> There is evidence that individuals and businesses dealing with government expect some knowledge of previous contacts on a particular issue. Data linking between agencies, with appropriate safeguards, will increasingly be required since the principle of 'enter once, use many times' can improve government efficiency and the service provided to citizens.

There are lots of issues in that, particularly if you look at a Web entry point for a citizen. Can you tell me how that general statement relates back to Centrelink? How do you envisage Centrelink further sharing information? Will that have to be done legislatively or will you effectively need an extension of the data-matching legislation?

Ms Treadwell—Given that Centrelink's whole approach is through customer service and support in terms of the way it integrates a whole range of government policies to give a holistic service to customers, we have done quite a degree of research into what our customers want and expect. Their 'tell my story once' is certainly a very strong request requirement, and probably led in part to the creation of Centrelink through the merging of a whole range of different programs and two government departments. In addition to that they want and expect secure management of their information. I think that, in our dealings with the Office of the Federal Privacy Commissioner, we have also found through his research that across the population there is some expectation that government agencies share information, but there would also be the expectation that it is well managed and controlled.

Centrelink has not been at the leading or bleeding edge of electronic information movements. There are many examples around the world of organisations that deal in the social security, welfare support and human services arena which have ploughed straight into much more open arrangements and transactions. I think that, whilst we have the expectations of our customers on one hand, as Pat was saying before, on the other hand we have the need to manage the risks to Centrelink's reputation associated with handling very important information as well as the maturity of our systems and the industry's capability to create confidence in the way technology plugs together to satisfy those needs. That is a long way of saying that our customers would like it as long as we can protect their information. We know that one of the best ways of doing that is to not let anyone in, but there is a trade-off in terms of how the information can be released. Our expectations are that we will seek customer authority to release that information on the legislation on almost every other occasion.

The other element within the Centrelink context is basically not creating more barriers than currently exist to a paper or other information transfer. We need to manage that which people currently expect and comfortably provide information, as John Meert was saying, over the fax. We will refer our customers to a range of other government and non-government organisations with a referral slip with particular details, so our challenge is to understand what the current processes are, how we can actually use technology to facilitate security and not put additional costs over that, both in terms of customer time and convenience as well as the technology cost to manage it. Therefore, we are doing it very slowly.

Senator LUNDY—Thank you. The paper goes on to talk about architecture principles and makes this statement:

A federated approach to government ICT governance, architecture and investment is appropriate in the Australian environment.

It goes on to talk about converging existing and planned systems and service channels. Can you provide a practical interpretation of what that means to Centrelink, particularly in the context of your vast database and the mainframe and hardware arrangements.

Ms Treadwell—Those words reflect the general concepts that are being considered by the CIO committee in the states as well as more generally across the e-government developments around the world. From a Centrelink perspective, we have pursued the concept that, if we can share some of the underpinning infrastructure across government agencies, we can collectively benefit by not having duplication of pipes and boxes—and, in fact, technology skills and capabilities. The big test then becomes that which is pertinent to the way the agency operates, and I think it is even more substantial in terms of the content of the customer processing information.

Senator LUNDY—Can I take a guess at the concept here, starting with Centrelink's hardware as a base. That hardware is potentially the location of data from other agencies to be accessed by them, albeit by software that could well keep barriers and lines between the different data sets, even though it could all be on the same machine. Is that where you are coming from?

Ms Treadwell—I suppose we are exploring that. We are exploring the issues around FedLink and Icon and all of those sorts of arrangements. When we start getting into software, it is certainly a means by which you can control access. It does not have to be physically separate, although it certainly gives a lot more comfort to those who are managing it.

Senator LUNDY—Yes, I know, but I am referring to this whole concept of data as an asset and, conceptually, one vast repository of data with different software accessing it from different points—in this case, say, different agencies. It might even be the case that no one agency has access to all of that collected data. That is the concept that I am trying to convey.

CHAIRMAN—Is the machine called 'Big Brother'?

Senator LUNDY—You said it, Mr Chairman, not I. I think it is a concept that is well developed around the world in terms of looking for efficiencies within architecture. My next question goes to something a little bit removed—Centrelink's investigation and decision to go

with open source solutions. Could you provide the committee with your observations about the relative security merits of open source versus proprietary software and the factors that have influenced your decision to explore those types of solutions?

Ms Treadwell—We are in the very early days of looking at open source software. That came as an opportunity in our major contract with IBM. In regard to exploring how this particular approach could benefit Centrelink, we are looking at cost efficiencies in fairly back office type arrangements. We are still developing our strategy on Linux. We will then know how to actually approach the market. We are supporting NOIE in pursuing how that might actually be applied across government. It will take us a number of years to not only contemplate but do any transitioning of particular types of transactions or arrangements within Centrelink.

Senator LUNDY—I have some more questions on that big database of Centrelink's. Do you currently hold any data for other agencies and departments? 'Store' might be a better word.

Ms Treadwell—We do a lot of work on behalf of government departments and therefore they may interpret their slice of our business as us holding information on their behalf. But we do not provide any independent servicing arrangements away from that customer or government program work.

Senator LUNDY—They effectively use your computing power and computing resources to provide for their needs.

Ms Treadwell—It is the whole package. The data is linked to the customer process that is linked to the business partnership agreement that we would have with a range of government agencies.

Senator LUNDY—Correct me if I am wrong, but I understand the data—and I know you are not affected by the same big IT outsourcing contracts—is always retained as an asset of the Commonwealth government, isn't it?

Ms Treadwell—Yes.

Senator LUNDY—Are there are laws or regulations that you are aware of that relate to where that data can be held—in other words, the physical location of that data?

Ms Treadwell—Not to my knowledge. Certainly a few years ago we explored that quite intently.

Senator LUNDY—In what context?

Ms Treadwell—In regard to outsourcing.

Senator LUNDY—And the potential of not having your data physically located on site?

Ms Treadwell—We looked at it. We considered the environment, and at that time I suppose one possibility was for an outsourcer to offer services across the globe as opposed to contained

within Australia. At that time, there was to my understanding no legislation that constrained that. It would be more a policy position.

Senator LUNDY—But Centrelink did not go down that path anyway.

Ms Treadwell—No.

Senator LUNDY—On asset ownership, does Centrelink own all of the hardware assets in your information technology or are some of them—

Ms Treadwell—Provided by other companies?

Senator LUNDY—provided by the vendors?

Ms Treadwell—We lease a lot of hardware and software, so the actual asset itself is owned by the company, with which we would have ongoing arrangements.

Senator LUNDY—That raises a whole series of issues about redundancy and obviously contractual difficulties that I do not think I have time to go into here. I know there are some of those issues already on the record. How do those ownership issues impact upon your security polices and how do you factor in issues like redundancy and disaster management, given that you do not own the asset?

Ms Treadwell—To take a piece that I can answer carefully, the disaster recovery and business continuity arrangements that we have in place have improved incrementally and substantially over time. Since preparing for the year 2000, we have done an awful lot of investigation and shoring up the disaster recovery processes and arrangements and recovery to a much tighter time frame than we had three or four years ago. The simulations that we have done over the last few years have also improved our procedures and controls. With regard to backup and support, the companies that we are leasing software and hardware from and that provide other products are deeply involved in the disaster recovery plans. They are used and have proven to be able to respond within minutes of notice being given from around the world, so that actually brings intelligence to solving problems as they arise, which, within a big IT capability such as Centrelink, actually does crop up now and again. With regard to the ownership issues, I cannot answer that specifically.

Senator LUNDY—I am happy for you to take it on notice and provide the committee with any observations, reflections or actions you have taken to factor that in.

Ms Treadwell—It will be in our plan.

Senator LUNDY—I do not know how affected Centrelink was by some of the worms and viruses recently, but has Centrelink decided to report to DSD any incidences or attacks that occur on your system? I would imagine this happens usually through email, in viruses and worms. I think the system is called ISIDRAS; it is effectively a voluntary system where agencies and departments can opt in to report incidences. Do you participate in that?

Ms Treadwell—We do report and we have reported on any category 4 level, or high level. Our actual approach within Centrelink is to be very open and engage the expertise where it lies around the Commonwealth, and in fact the private sector as well. It is in our interest that we find out what is going on in other parts of the world and also let others know. With regard to virus management, that is being stepped up quite a bit. We regularly report to our board about the number and types of viruses that get stopped. Certainly, we have an environment that probably protects us a bit more than some other organisations, so the quantum of viruses is low compared to other organisations that might have a more popular type of software in place.

Senator LUNDY—Which software do you have?

Ms Treadwell—We use Lotus Notes and a whole range of other software.

Senator LUNDY—I thought it would be Microsoft.

Mr Fegan—As part of the gateway we have some intrusion protection software and stuff like that.

Senator LUNDY—It is always worth asking the question. I have so many questions, but I will ask one more. On the information management group, I know of another initiative that the government has begun relating more to critical infrastructure protection and, again, another series of committees. How are Centrelink engaged in that, if at all? From the information I have, I am not sure how far the critical infrastructure protection committee and advisory council extends into agencies and departments. Could you give me an insight into your involvement there?

Ms Treadwell—NOIE will be able to help you with the integration and the link when they are here tomorrow. From the CIO committee perspective, we do not want our people being asked to advise and contribute to certain groups that could be rehashed into another one. NOIE can advise you on that. Centrelink have responded to requests for information which we have been compiling on critical infrastructure, but obviously it operates at a much more significant level than a service delivery agency would.

Senator LUNDY—Can you remind me how many citizens Centrelink serves throughout the country?

Ms Treadwell—We have 6.4 million current customers.

CHAIRMAN—Why haven't you applied for Gatekeeper certification?

Ms Treadwell—Gatekeeper certification is a very complex piece of technology and is mainly being used for companies and businesses, so the issues for Centrelink are its complexity and the driver for it. The CIO committee working parties are looking at the way in which authentication can be applied to both businesses and individuals, and this is where we would hope that potentially there is a facility through which Centrelink can engage rather than having to replicate something that complex across multiple organisations. We are looking at the types of transactions that require higher levels of security and management than, for example, providing information as to where the local neighbourhood house is. We believe that there are a range of services and transactions that would require varying levels of authentication and security.

CHAIRMAN—My colleagues discussed informed consent with you. Let us say that CSA had a custodial parent client and the non-custodial parent—who you were paying an unemployment allowance at a different address—had done a runner, and the custodial parent advised CSA that they knew where the former husband or partner or whatever was. You are not telling me that you would go to this person and ask them for informed consent before you cut off their benefits?

Ms Treadwell—No.

CHAIRMAN—You will not mind if we put any further questions in writing, will you, to save you coming back?

Ms Treadwell—We would be more than happy to answer those.

CHAIRMAN—Thank you very much.

[12.17 p.m.]

McEWIN, Ms Marion Kathleen, Assistant Statistician, Policy Secretariat Branch, Australian Bureau of Statistics

PALMER, Mr Jonathan James, First Assistant Statistician and Chief Information Officer, Technology Services Division, Australian Bureau of Statistics

CHAIRMAN—Welcome. Thank you very much for coming and thank you for your submission, which we have released for publication. Do you have anything you would like to briefly add before we ask the questions?

Mr Palmer—No.

CHAIRMAN—You have talked in your submission about ABS culture strongly valuing information security. I note that ANAO, when it audited 10 agencies, gave you a very good rating out of very good to very poor. How did you manage to develop that culture and over what period of time?

Mr Palmer—I guess there are many facets to how we manage our culture. It starts when people arrive and the explanations we give them of the role of the organisation and the undertakings that they have to sign, including an undertaking of secrecy, I think, under the Census and Statistics Act—

Ms McEwin—It is called fidelity and secrecy.

Mr Palmer—That focuses the mind of a new starter, that they have actually signed something that says that if they do not meet those obligations they can be imprisoned or fined. We follow up with induction processes and training, visible security around our physical premises and the allocation of user IDs and passwords. Then there are elements of our corporate plan which I think make this aspect of our culture quite clear and important. Our education programs communicate outcomes of things like the ANAO audit to all staff to reinforce the importance. Many of our staff might have to liaise with respondents to surveys, so these issues come up. People ask on what basis they have to give information and how is it protected, so many of our staff would be well versed in our answers to those questions. They are a number of the elements that maintain the culture that we have.

Ms McEwin—And when we are disseminating our statistics in the form of compilations and tabulations, we are required to make sure that we do not divulge any individuals within those, particularly if the tabulations are very detailed ones. So people are well aware of the procedures that we have had to develop and the methodology that supports those procedures, as well as their application. They are working with this every day in their work and it is not something that is remote from them, and the culture is built up as a consequence of that.

CHAIRMAN—I hear you, but I also remember 15 or 16 years ago as a supplier of information to ABS—I was not a client; I did not receive the information, I had to supply it—receiving a survey form which really amounted to a de facto profit and loss statement stated in

different terms than we would have kept our books and being threatened with death and destruction if I did not fill the blasted thing in. Have you changed that aggressive approach at all?

Ms McEwin—I guess we would like to think so.

CHAIRMAN—I did not fill it in, by the way. It was too intrusive.

Ms McEwin—One of the points you made was about information being asked for in a form that was not consistent with the way in which you had kept it. Through our development and testing procedures, it is our goal to try to ensure that we ask questions that are consistent with the way that people keep their records. When we are discussing with providers of our information and talking them through the questionnaires that we send out, if we are trying to persuade them that it is important to fill in this particular questionnaire, we certainly tell people that careful estimates are appropriate and that we will do what we can to help them fill the form in.

If we are unable to get information, then we do have power to direct people to provide that information. It is that power that I think you are referring to that could lead to prosecution if people fail to respond after a notice of direction. But we rely—as I think we said in our submission—very much on willing cooperation. It is mission critical to the bureau that we have a cooperative community that is providing information to us rather than our having to use any threat or force of law. In the main, we have found that we get good responses to our surveys, but that does not mean that we do not need to keep working at managing our relationship with our providers and make sure we are asking reasonable questions.

CHAIRMAN—You said in your submission that you had your firewall infrastructure certified by DSD. Have you used DSD for any other purposes?

Mr Palmer—We maintain quite a close relationship on the information security side with DSD, as well as the formal certification process. We will talk to them about any planned changes to our environment and bounce our ideas off them. Then there will be some interaction with them, no doubt, on various committees. At the working level, we have a couple of people who call them every now and then and talk about what we are doing and get advice and ideas.

CHAIRMAN—I would have thought that you were a very important privacy and security agency in terms of assuring the public that, when they give you information, it stays where it is supposed to stay. Have you had many breaches? If so, could you tell us about them?

Mr Palmer—I do not know of any breaches. Are you asking specifically about our IT infrastructure, our firewalls, gateways and things?

CHAIRMAN—Has any data been inadvertently released, or have people or organisations been able to break into your systems to obtain statistics or data on individuals or companies?

Mr Palmer—No, not to our knowledge. From the very start of our external links to the external world—which we avoided for a long time; we had no links, just an air gap, and we were connected to no-one. When we moved to even the most rudimentary of web site presences, we were DSD certified from the very beginning. I think we claim to be the first, although I

know Centrelink will argue whether it was provisional or final certification. We have certainly been certified from day one.

There have been tests of our infrastructure which have shown us to be very robust. In the ANAO audit they managed to change the content of an error file, so I guess there was a demonstration that a file that we thought was protected was not. But we certainly do not know of any successful attacks that have allowed people to take away statistical data or sensitive data that we did not want to expose.

CHAIRMAN—I believe you intend to use FedLink.

Mr Palmer—Yes.

CHAIRMAN—Can you tell us how you intend to use it?

Mr Palmer—I am not clear on whether we are already using it, but there are agencies that currently send data to us—

CHAIRMAN—Such as the tax office.

Mr Palmer—The tax office is one and I think Customs might be another. We regard FedLink as a good solution to that need to have these agencies be able to send us data in a secure way.

Senator LUNDY—To what extent do you use Gatekeeper and the public key infrastructure?

Mr Palmer—If we use it at all it would be very minor. The scale and the scope of the business we do online does not really warrant the issuing of digital certificates, so we do not use it at the moment.

Senator LUNDY—Can you envisage a need for it in the future?

Mr Palmer—I am not sure. From a respondent convenience perspective, if it were convenient for the survey respondent to use the Gatekeeper certificate as their way of authenticating and dealing with us online then I think we would want to use it. From an ABS perspective, we would have to look at the types of risk we were trying to manage. It is interesting that the risks we try to manage are not quite the same as those of Centrelink or ATO. People tend not to fraudulently lodge statistical returns on behalf of other people. We just do not have the same need for non-repudiation that Tax might.

Senator LUNDY—What about attacks via email worms and viruses? Can you give us some general feedback about your countermeasures and whether your department reports to DSD's ISIDRAS system?

Mr Palmer—I do not know, but I am quite sure that we would report. We are certainly aware of the appropriate reporting mechanisms and would use them if required. I do not know whether we have made any reports. We have a range of measures to scan for viruses and monitor incoming traffic. To date they have proven very robust—in part because we operate in a somewhat different environment to many who are also Lotus Notes shops.

Senator LUNDY—Do you think that makes a difference?

Mr Palmer—I think it does. It is a less popular target environment. Perhaps the nature of some of the controls we have been able to build in are another level of protection. I have asked before whether we have had any attacks that have impacted on organisational efficiency—other than on an individual whose work station has had to be rebuilt—and I know of none that has been of that scale. So we have fared quite well, but we are attacked all the time.

Senator LUNDY—People try and get in all the time?

Mr Palmer—Yes.

Senator LUNDY—As far as your outsourcing arrangements go, can you describe in general how ABS manages its sourcing of IT hardware, software and network needs.

Mr Palmer—We are largely self-reliant; self-servicing. We own and operate our own IT infrastructure and we own the vast bulk of it and operate the vast bulk of it. We were not one of the parties to the outsourcing clusters.

Senator LUNDY—How would you describe your model of procuring your needs?

Mr Palmer—Our procurement model is very much sourcing aimed at value for money. We will, whenever we have to procure anything significant, first and foremost think about how we can create a good competitive environment and get value for money, so we make a lot of use of tenders and RFPs. We draw on advisory services like Gartner to establish whether offers we are being given represent value for money. We do a lot of work with our existing vendor relationships so we try and create relationships where they understand what we are trying to do and come to us with good offers so that we can continue to work with them.

Senator LUNDY—As far as those ongoing relationships go, how do you factor in new and emerging issues like critical infrastructure protection, the heightened emphasis on e-security and all those kinds of issues? Is that something you negotiate as they come up or do you find yourself having to renegotiate aspects of your contracts?

Mr Palmer—I think they are things we deal with as we go along. Because our model is fairly simple—we will buy a product or a service—it is not a highly bundled thing with lots of complexities. It does not seem to be a problem for us.

Senator LUNDY—So you would say you would retain full strategic control of your IT services and systems?

Mr Palmer—Very much.

Senator LUNDY—I have one more question about archiving. I am not particularly familiar with the sorts of information and data assets that you have but I know you produce a vast array of reports, some of which you charge for and others which are publicly available. Do you have a uniform or standard archiving system for electronic data of that nature?

Mr Palmer—We are working on one. We have just signed off on a new corporate data retention policy which attempts to give more guidance to our various areas as to what data should be kept and for how long. In that policy, we have a class of data that I like to call 'retain forever' but I think we call it in the policy 'retain indefinitely'. Some of the information we can retain indefinitely by putting it in a system that is always being operated and so we know the data is there and safe every night, and then when the system is upgraded the data structures are upgraded. Our core repository there is a thing we call the ABS DB, which is a large database. Some data is effectively archived by putting it into there. It does not mean it is taken off site or written to some other medium. People can put it there and not worry about it over the long term.

But we are also at the moment working on decommissioning a mainframe which has some data on it that we would like to keep, possibly indefinitely, and we are working on XML schemas that can be used to describe that data so we can take it away from its current processing environment—say a SAS program or something—and still be confident that we know what the data is and what its structure is. We are still working out where and how we will store the data. We are obviously interested in any standards that are emerging in that area.

Senator LUNDY—I was referencing some of the strategies outlined in this new governance for the investment framework report. What is the ABS's involvement on the CIO committee or any of the associated committees within that structure?

Mr Palmer—Dennis Trewin, the Australian statistician, is a member of the IMSC. I am a member of the CIO committee and I am involved in three or four of the working groups. I say 'or four' because one of them has not yet been established. I am involved in the customer authentication working group. There is another working group to do with identity management of Commonwealth government employees and contractors; I am on that one. There is another working group which is to do with service delivery channels and that is the one that I have not yet participated in. I am trying to think if there was one other. So I am involved in a number of the working parties.

CHAIRMAN—In the event of a major disaster—that is, losing your mainframe—what sort of disaster recovery plan do you have in place?

Mr Palmer—We have different plans for different elements of our infrastructure. In some cases, we have plans that rely on the fact that we have redundancy facilities. We might have servers in state offices that can be brought to bear across the network. In some cases, such as our mainframe, we have an arrangement with the supplier that will allow us to get replacement hardware in a reasonable time frame.

CHAIRMAN—Is the data held in another secure environment as well?

Mr Palmer—Yes, the data itself is—

CHAIRMAN—If the building blows up, if a cruise missile takes out the mainframe, would you still be able to have access to your data?

Mr Palmer—Yes, you will lose some work in progress. You will lose what was not backed up and taken off site since the last window, but the core information assets of the ABS will be safe and robust.

CHAIRMAN—Including your archives?

Mr Palmer—Yes.

CHAIRMAN—Thank you very much. If we have further questions, can we put them in writing rather than ask you to come back?

Mr Palmer—Sure.

Proceedings suspended from 12.38 p.m. to 2.03 p.m.

DARK, Mr Gregory, Assistant Commissioner, Australian Taxation Office

FARR, Mr Gregory Douglas, Second Commissioner, Australian Taxation Office

VOHRA, Mr Chander, Assistant Commissioner, Trusted Access, Australian Taxation Office

CHAIRMAN—Welcome. Thank you for your submission, which we have published. Do you have a brief opening statement to make before we move to questions?

Mr Farr—I would like to make a brief statement. The Australian community has a legitimate expectation that information collected by the ATO is stored, managed and transmitted securely and that the privacy of individuals is maintained. We take that extremely seriously. I could mention a number of initiatives that the ATO have undertaken over the years where we have been at the forefront of a whole range of electronic initiatives, security initiatives. For example, we were the first Commonwealth agency to attain DSD accreditation for its Internet gateway to a protected level. To do this, of course, we had to implement DSD approved procedures in managing risks. We were the first agency to attain full gatekeeper accreditation for our certification authority in May 2000. About 80,000 large businesses now interact with the ATO for the lodgment of their business activity statements using the keys and digital certificates issued.

We obtained provisional highly protected certification for our upgraded Internet gateway in February 2001, and we were the first Commonwealth agency to achieve this distinction. We have of course been involved with other agencies in the development of FedLink. Along with DEWR, we have developed the business authentication framework for validation of ABN-DSCs. We also have an approved e-business strategy for the ATO, which provides a consistent approach for managing the risks from the Internet while implementing our online systems. The approach that we have adopted is fully consistent with the guidelines provided by the ANAO, NOIE and DSD.

Perhaps most importantly, in recognition of the importance of Internet security, the ATO has formed a trusted access branch, headed by an assistant commissioner—Mr Vohra—to enable management of all issues relating to security in a proactive and integrated manner. Currently employed in Mr Vohra's branch are about 60 staff dedicated to that task. Notwithstanding these very significant and ongoing efforts, the potential for compromised security cannot be totally overcome. Incidents will and have occurred. It is a common feature of the literature that I have read on this topic that it is a question of when rather than if an incident of this nature occurs and, therefore, it is equally important that these incidents are promptly and professionally handled when they occur.

I will mention one such incident to give an example of how the ATO goes about that. Shortly after the implementation of the ABR, the ATO received advice that a person had been able to access an incomplete application of a non-related company. They had retrieved a partially completed application which related to another person. As soon as we became aware of that problem, we identified the area of risk; we removed any data that could have also been at risk of being exposed; we removed the functionality from that part of the system from public access;

and we commenced urgent work to establish what had caused the problem. The client was immediately notified and offered a replacement TFN and had all other TFN information blocked. The Privacy Commissioner was notified of the incident and how we responded. The Privacy Commissioner commenced an investigation shortly after that, and the advice from him said at the conclusion, 'I am satisfied with the explanation you have given about the circumstances surrounding this incident and the action you have taken.' We clearly take incidents of that nature very seriously, including when they are caused not by the ATO but by factors outside the ATO.

Finally, we need to remember that in any electronic dealing between the ATO and the community a significant part of the infrastructure in the chain is not controlled by the ATO. While the ATO and other Commonwealth agencies are very aware of security vulnerabilities and of the latest developments in combating them, large segments of the general community who access online services are not so well informed. In many cases, the most serious vulnerabilities exist not on ATO infrastructure but on the client's PC or desktop. It is a major challenge for the ATO and Commonwealth agencies generally to bring users to a similar level of understanding and care as that which we apply ourselves. In the meantime, ATO's strategies will continue to be directed towards that.

In framing the ATO submission, it was difficult to know what level of technical depth to go to. I hope that, between my colleagues and I, we will be able to offer assistance to the Commissioner at all levels—from our overall policy and approaches to, if necessary, the in-depth technical architecture of our security measures. For obvious reasons, if we do move into the more specific and detailed discussions around the ATO's security architecture we would prefer that not be done in an open hearing. That is all I really wanted to say by way of an opening statement.

CHAIRMAN—Thank you. In your submission you said:

> The Commonwealth Protective Security Manual requires people granted access to security classified information to hold a security clearance commensurate with their level of access. The majority of ATO staff with access … either have a security clearance or are undergoing vetting.

Where do you stand with that?

Mr Farr—The pre-engagement checks that all staff, before they are given access to any information in the tax office, are required to go through—police checks and other character checks—provide a security level of 'in confidence'. So all ATO staff are cleared to at least in confidence level, which is in essence taxpayer data level.

CHAIRMAN—Is that formal clearance?

Mr Farr—I am not sure what you mean by formal clearance.

CHAIRMAN—The Protective Security Manual requires a successive level of certification of clearance, and I want to know if they are all signed off or if they are waiting on the checks and approvals.

Mr Farr—At the in confidence level, all the staff who have access to data have gone through all those checks and have been ticked off.

CHAIRMAN—How about the other classifications?

Mr Farr—At the 'highly protected', 'secret' and 'top secret' levels we have an ongoing program of having people secured to those levels.

CHAIRMAN—Yes, but how far behind are you?

Mr Farr—I can give you those details. While I am getting those figures, let me say that part of the problem is that we have actually flooded the providers with requests that they have to clear, so the slowing down is not from our point of view.

CHAIRMAN—Mate, we have had all kinds of excuses from more than one Commonwealth agency on why security clearance is not up to date.

Mr Farr—Currently we have 2,521 people secured to 'highly protected' or above level. We have 1,148 who are currently with providers going through the checks, and we still have about 2,400 to go.

CHAIRMAN—Shivers! So you really are pretty far behind.

Mr Farr—I do not—

CHAIRMAN—I would think the numbers speak for themselves, Mr Farr.

Mr Farr—As I said, we have made a concerted effort to actually get all of the staff through there but the security providers who actually provide that service are unable to go any quicker. We have looked for alternative suppliers and there are none. We would like to be further ahead than that, but I am not sure there is much more that we can do in the absence of that capacity by the providers.

CHAIRMAN—In your submission you also talked about contractors. You said:

Contractors who have access to classified information are subject to the same pre-engagement character checks and induction training as ATO employed staff—

and 'security awareness is maintained' and all that stuff. Are you confident that your contractors, subcontractors and sub-subcontractors have up-to-date security clearances and checks?

Mr Farr—The short answer to that is yes. All the contractors that we employ go through the same checks as if they were ATO staff.

Mr Vohra—Another thing is that before these staff get access to the required level of information, those security checks should be in place otherwise they will not be able to access the information which they are supposed to have as a part of their business.

CHAIRMAN—That is contractor employees as well?

Mr Vohra—Yes. For example, we ensure that the EDS staff have the required security clearance before they can handle ATO information.

CHAIRMAN—You outsource a fair amount of your information technology, don't you?

Mr Vohra—Yes.

CHAIRMAN—In doing that, your software design requires people to have, I would have thought, pretty sophisticated clearance levels in order to be able to design the software.

Mr Vohra—There are certain variations. Not all the staff require a highly protected level of security clearance.

CHAIRMAN—Sure. I understand that you could sit and write code day after day and not have a clue what you are doing. Are you telling me that all the contracted staff who need high security—those who have to understand the system architecture and the software requirements that they are working into, how the firewalls work and all of that—are cleared?

Mr Vohra—Yes. They are all cleared.

Mr Farr—To make sure we are all on common ground: although we outsource a large portion of our infrastructure, our application development is in-house. We have not outsourced our application development.

CHAIRMAN—So all your software is done in-house.

Mr Dark—It is performed in-house but we have contract assistance. It is controlled and managed in-house as opposed to being managed by an outsourced provider.

CHAIRMAN—Your basic systems design is done in-house not by an external contractor?

Mr Farr—Yes.

CHAIRMAN—I did not realise that.

Senator LUNDY—What software do staff use for their desktops?

Mr Vohra—Microsoft XP is what we have now on our desktops.

Mr Farr—We have a whole range of other software. A lot of it is custom built. We have about 900 staff in our applications development branch, so a lot of the software that we use is purpose built for our applications.

Senator LUNDY—I will come back to that.

CHAIRMAN—You say in your submission that all ATO data sent over Australia-wide networks of desktop personal computers is encrypted immediately prior to entry to the networks and decrypted immediately after exit. Has DSD tested that?

Mr Vohra—The ATO uses DSD-approved encrypters at both ends. We do not use any encryption products that have not been approved by the Defence Signals Directorate.

CHAIRMAN—They have checked it all?

Mr Vohra—Yes.

CHAIRMAN—And that is true of the public key infrastructure encryption?

Mr Vohra—Yes, it is true of that as well.

CHAIRMAN—So you have used DSD for that, you have used them for FedLink and for Gatekeeper. Do you use them for any other purposes?

Mr Vohra—We use DSD-approved firewalls. They are a main component of our Internet gateway. Then there are certain monitoring tools that DSD has approved—what type of monitoring should be in place when the Internet is connected. Everything is in accordance with DSD guidelines.

CHAIRMAN—Beyond that, have you used them as an inspector-general, if you will, to test the reliability and security of all those things?

Mr Vohra—The organisation which tests the operation of this particular infrastructure—that is where the actual reliability is tested—is on the DSD's list of approved service providers. From time to time, we undergo some external analysis through the approved organisations, and that analysis tells us whether we are doing all right or whether we need to improve something. It is more in terms of, for example, testing the Internet and being able to see whether or not someone can compromise our systems. We go to that level of testing.

CHAIRMAN—I am advised that a submission from the office of the federal Privacy Commissioner and the Australian Unix Users Group mentioned an incident in June 2000 in which a user of the Commonwealth GST Assist web site was able to get access to the banking details of 17,000 businesses. Can you tell us about that?

Mr Dark—Yes, I can. That web site was not an ATO web site. It was a Treasury web site. It was not under our control. It was the web site that was dealing with the $200 cashback certificate. It was not one of ours; it was Treasury's.

CHAIRMAN—Then how did they get the ABNs?

Mr Dark—An ABN is a public number. It is available publicly.

CHAIRMAN—Yes, but lists of ABNs are not.

Mr Dark—The ABN public site, which is operated by the Business Entry Point, is the public portion of the Australian Business Register—and it is public.

Senator LUNDY—The Business Entry Point web site has previously dealt with issues relating to the privacy of the ABNs listed on it—and the tax office was involved in that—because you are the original source of that data. Were you the source of the original data used on the Treasury web site—either directly or indirectly through the Business Entry Point site?

Mr Dark—I cannot recall the circumstances, but I believe that that information was provided by the companies themselves in the process that they went through with Treasury.

Mr Farr—We can check that, but that is my recollection as well: it was on the application form for the grant, which was then collated by the Treasury web site.

CHAIRMAN—Indirectly would have to be right—wouldn't it?—since you have issued all the ABNs.

Mr Dark—That is correct.

Senator LUNDY—I would like to follow up on that, if I may, because it relates to an earlier incident. For the committee's benefit, could you explain the outcome of that previous incident relating to the Business Entry Point and the sale of data relating to companies and the ABNs—I think it was Dun and Bradstreet at the time. I know that it had repercussions for you, and that it meant Tax had to change their way of dealing with that data and how you shared that data. That is my memory of it.

Mr Dark—It is a long time ago, but I could do it to the best of my recollection, if you like.

Senator LUNDY—If you need to you can correct the record later.

Mr Dark—My understanding is that there was a body of records—I think about 10,000—provided by Business Entry Point to Dun and Bradstreet, I believe, as a testing exercise because Dun and Bradstreet present various types of public information about companies and, as I recall, they wanted to make sure that our promises regarding incorporating ACNs within ABNs were working and that they could keep their web site or register correct with our details. There were all sorts of allegations about the sale of that information. I do not believe that that information was sold. I believe there was a facility fee for preparing whatever the medium was that was passed between the Business Entry Point and Dun and Bradstreet, but it certainly was not them saying, 'Each record costs you 10c, so here's an amount.'

Also, to my recollection, when the Privacy Commissioner looked at it he found that the disclosure was within the law. As a result of going through the process of examining that disclosure, the commissioner asked us to upgrade some of the words in the privacy statement in the application for an ABN, which we did. I think that is about the size of it. That is my recollection. At that stage the ABN law provided for an entire ABN record to be disclosed to the public, on request. Shortly after that, government amended the disclosure arrangements to separate a certain amount of the register, which was public, from the rest, which was not public and was only available under certain conditions to other government agencies.

Senator LUNDY—My recollection is similar to that, but I think I actually got on the public record, from the agency concerned, that it was their intention to try to sell that data. I think you are right in the sense that it did not actually happen.

Mr Dark—I really cannot answer for their motives or whatever, but the intention was that.

Senator LUNDY—I think it was one of those learning moments for everybody. What happens now in terms of the data you collect? Obviously, you do share that data with kindred agencies involved in interfaces with businesses. Can you explain the terms and conditions under which you can share that information with other agencies and departments?

Mr Dark—Section 30 of the ABN act, along with some regulations that go with it, authorises disclosure of non-public information to other agencies. Before we enter into an agreement with another agency to supply them with ABN data we go through a series of checks. The first is that they comply with the legal requirements to be entitled to receive the information—that is, it is for legitimate purposes of their agency. The second is that they meet a number of conditions in regard to providing security for that information and what happens if they do not. We do this by means of a memorandum of understanding which is signed prior to the provision of data. That memorandum very clearly sets out the law and the protections available to that data under the law and makes sure that they are aware—they should be—of all the arrangements around the provision of that data and what they can do with it.

Senator LUNDY—Have you had any other instances like what happened with Treasury occur, where data that you have shared under an MOU has subsequently found its way into the wrong hands, either inadvertently or consciously?

Mr Dark—There has been nothing that I know of, and I probably would.

Senator LUNDY—EDS provide you with quite an extensive vertically integrated service provision, albeit not applications development. What contractual environment ensures security via that third party?

Mr Vohra—That is part of our service level agreement with EDS. EDS staff would be held responsible in the same way that staff of another agency would be held responsible. The Privacy Act 1988, and its subsequent amendment, is applicable to EDS as much as it is applicable to any other agency.

Senator LUNDY—Is that because the act is evoked, if you like, within the contract?

Mr Vohra—When the contract was signed there was only the 1988 legislation. At that point in time we knew that there would be new business requirements that would require greater emphasis on privacy and all that, so that was built into the service level agreement with EDS.

Mr Farr—But it is worth noting that, having agreed with EDS on the arrangements, Mr Vohra's people work with them to ensure that they are complying, as opposed to just leaving it up to them to do that. They have the same level of governance and scrutiny over those issues as ATO employees do.

Mr Vohra—For example, we can access the information, audit the information and ensure that they comply with all the requirements.

Senator LUNDY—Is any data that is an asset of the Commonwealth on computers that are not physically located in Australia?

Mr Vohra—EDS do backups of our information from time to time. To the best of my knowledge it is stored off-site in Australia, but I would need to confirm that.

Senator LUNDY—But it is still physically in Australia. Could you check that for me?

Mr Vohra—Yes.

Senator LUNDY—Are you aware of any laws determining that that must be the case or any laws preventing Commonwealth data assets from being stored offshore?

Mr Farr—I am not aware of any. I am very confident in saying that none of those backups are stored offshore. We might be able to check that before we finish here.

Senator LUNDY—I am asking the question because, if there are data assets held offshore, they are not within this jurisdiction and therefore we cannot be confident that they are covered by Australian laws.

Ms PLIBERSEK—There seems to be a varying use of FedLink between departments; some use it more, some use it less. How much do you use it, what do you use it for and does it suit your purposes?

Mr Vohra—The development of FedLink took considerable time. During 2000 we had a pilot run. The reason for FedLink was that—

Ms PLIBERSEK—You ran the pilot in 2001?

Mr Vohra—The pilot concluded in 2001. We have subsequently been converting that pilot into a production system. The objective of FedLink is to provide secure communication between various Commonwealth agencies to enable them to exchange information up to a protected level. The initial FedLink design required certain very minor changes at the agency's Internet gateway. Designs were tested, and one of the critical things was the installation of digital certificates on those boundary devices. The infrastructure is in place now, so the agencies which want to communicate with each other have only to do very minor work and they can start being on FedLink. We have been on FedLink since 14 December 2002. Currently, we are very close to initiating our testing with AUSTRAC. They are also on FedLink, so they will probably be the first agency that will come and work with us. In terms of the broader use of FedLink, we intend migrating other agencies which connect to us through ISDN and other links to use FedLink, as it provides a single communication channel. It assumes that within the agencies there is a certain level of existing security, as checked by DSD. But, once that is done, it will allow us to communicate with other agencies for a range of applications.

Ms PLIBERSEK—When do you expect to start using it?

Mr Vohra—We are ready, but AUSTRAC would be the first agency which—

Ms PLIBERSEK—You are waiting on AUSTRAC?

Mr Vohra—Yes. We are working with them, so we should be connected to them through FedLink very quickly. Another thing is to migrate our other system through this link, then the existing link would be the next thing. But the first point is to ensure that we are connected to them through that.

CHAIRMAN—Are private binding rulings only made available to the individual who applies?

Mr Farr—They are only made available by us to the individual who applies.

CHAIRMAN—That is the question; I should have clarified that.

Mr Farr—There is a precis of it so that the ruling, without the details identifying the individual taxpayer, is made available more broadly so that people can see what we are ruling on. From our point of view, a private binding ruling only goes to the person or their accredited representative—their agent or solicitor.

CHAIRMAN—Where do you publish both the circumstances and the ruling? If I come to you as an individual and say, 'This is the way I've treated my funds. Could you give me a private binding ruling on whether that meets certain taxation criteria?' and you come back and say, 'Yes, under these conditions,' is that whole scenario—minus my name, ABN number and whatever else is involved—published?

Mr Farr—Yes, it is on the web site, but it is probably a more stringent check than that. People go through it to make sure that there is no information on the web site that could identify the taxpayer. But, by the same token, people can see what it is that we are ruling on. From a transparency point of view, they can see that these are the rulings we are issuing.

CHAIRMAN—This has nothing to do with this hearing, but I am fascinated. You say that that is the case. Has that led to some problems, with people reading private binding rulings and assuming that they will be clean without applying for one themselves?

Mr Farr—I am not aware of any problems that it has caused but, in a sense, we are damned if we do and damned if we do not. If we do not, people will say, 'What are you ruling on? There is no transparency for the community.' If we do, people might say, 'That applies to my circumstances.' But in those circumstances they should get a private binding ruling, in which case they can say, 'But mine's different to what seems to be on the web site,' and that is the intention of it.

CHAIRMAN—But public rulings are clearly public.

Mr Farr—Yes, they are.

CHAIRMAN—Once you make a determination, it is published and people can be assured that, if they do exactly the same thing under the same circumstances, the same rules will apply and they will be treated the same. If they are not, they have recourse.

Mr Farr—Yes.

CHAIRMAN—But the private binding ruling only has application to the individual or individual company, trust or whatever legal entity that applied for the private binding ruling.

Mr Farr—That is right.

CHAIRMAN—And you still publish the information. Are you asking for it? Again, it has nothing to do with this hearing.

Ms PLIBERSEK—I am on their side. People want to know what decisions are being made. You would get into all sorts of trouble if you were making private rulings and not telling anyone what they were.

CHAIRMAN—I accept that, but it probably gets you in trouble too.

Mr Farr—Senator Lundy, in answer to your previous question, my advice is that there is no data stored outside the country. The contract says that the data and all facilities must be located in this country.

Senator LUNDY—Thank you.

CHAIRMAN—In 2001, the ATO took part in an ANAO performance audit of Internet security. What was the outcome of that audit with respect to the ATO? Did you get a very poor, a medium or a very good rating?

Mr Vohra—I think the ATO was one of the larger of the 10 agencies that were audited as a part of that exercise, and we received a reasonably good report compared to the other agencies. All the ATO's web sites were extensively studied. We received only minor suggestions, and we had those implemented soon after that. What we have in place now compares with the ANAO's better practice guidelines, so we compare very well with all 40 points mentioned against various systems, including these web sites.

CHAIRMAN—Mr Farr, I think you said that you have 900 staff involved in information technology.

Mr Farr—Yes, in applications development.

CHAIRMAN—Out of how many ATO staff in total?

Mr Farr—Around 20,600.

Senator LUNDY—Going to one aspect of your submission—'Measures to Protect Information Being Transmitted by the ATO'—I notice you say:

The ATO employs email filtering to reduce the incidence of spam, to detect viruses, trojans and worms and thereby ensure as much as possible that its networks are available to perform its work.

You go on to say:

The ATO applies the latest security patches to its software to mitigate the risks of denial of service and trojan attacks.

What is the process of identifying security breaches and the availability of patches, and have you had any incidents of a time lapse between the identification of the security breach and the availability of patches from a software company?

Mr Vohra—Yes. We focus on two areas. The first area is the Internet area, where we basically rely on DSD, AusCERT and other leading organisations. We keep up a very proactive monitoring of all the possible sources of these vulnerabilities. Within the Trusted Access Branch, we have a team purely looking after such vulnerabilities, and they assess whether or not they are applicable to the ATO. If they are applicable to the ATO, they talk to these concerned areas straightaway and keep on following up until the patches are applied. In many cases, there is a time lag between the vulnerability being discovered and the patch being made available. We cannot minimise that particular time lag but, over a period of time, we have observed that such time lags are reducing considerably, and we have very strong procedures in place to apply these patches as soon as possible. EDS are responsible for our internal systems, like all the file and print servers and the internal network, and our experience with them is that they are quite proactive in the whole process. The procedures are quite well defined. I have the statistics in terms of how many patches we have applied over the last 12 months.

Senator LUNDY—It would be excellent if you could provide them to the committee.

Mr Vohra—I would like to provide them separately. I have those figures with me.

Senator LUNDY—Thank you. We would like to get those. Does the ATO use DSD's ISIDRAS incident reporting system?

Mr Vohra—Yes. All the incidents that we record on our Internet gateway exactly map the categories of incidents that DSD have given us. We have access to their information, and we keep on updating that particular database. In fact, the vulnerability assessment team within our branch is responsible for ensuring that we keep access to the information in that particular database. We do not only track it, but we record incidents exactly so that they can be picked up and mapped onto that database without any extra work.

Senator LUNDY—Was the ATO affected by the SQL Slammer virus in January of this year?

Mr Vohra—No. The ATO was not affected because we are very strict on our policy in terms of what types of attachments can come into the organisation, so we have been able to handle all such situations quite effectively.

Ms PLIBERSEK—When you say that you are strict on the types of attachments, do you mean that you have a policy requesting that your staff do not get personal emails at work, and therefore do not get attachments, or do you mean that you have an automated way of preventing those attachments breaking through your firewall?

Mr Vohra—We have a double gateway policy loaded. It does not allow in certain types of executable files that could contain potential viruses and such vunerabilities. All mail is scanned at the gateway to detect whether there are any unacceptable attachments. We do not let those messages come in.

Mr Farr—It is the latter rather than the former.

Mr Vohra—Yes.

Mr Farr—It is an automatic monitoring system.

Mr Vohra—Yes. We let the user know that the message has been blocked.

Senator LUNDY—I do not know whether you can answer this now, but my memory is that the SQL Slammer bug did not require an email to be opened, so I am not sure how directly relevant attachments are to it. But, do you have SQL servers, meaning that you were potentially vulnerable?

Mr Vohra—Actually, I was not answering that question with respect to email. That is a separate question. In the case of SQL Slammer, we were depending on Microsoft to provide us with the patches.

Senator LUNDY—So you had the patches in?

Mr Vohra—Yes. Our experience is that Microsoft are now responding much more quickly with respect to these patches. We use SQL servers extensively, so we applied the patches to them.

CHAIRMAN—Thank you very much. As I have asked everyone else, I assume that if we have further questions you would prefer that we put them to you in writing rather than asking you to come back?

Mr Farr—Absolutely.

CHAIRMAN—Thank you very much.

[2.45 p.m.]

McLAREN, Dr Ron, Assistant Secretary, Information Management and Technology Strategy Branch, Business Group, Department of Health and Ageing

SEITTENRANTA, Ms Eija, Assistant Secretary, Technology Services Branch, Business Group, Department of Health and Ageing

SUTTON, Mr Gary Leslie, Director, Information Strategies Section, Information and Communications Division, Department of Health and Ageing

WOODING, Dr Robert Edward, First Assistant Secretary, Information and Communications Division, Department of Health and Ageing

CHAIRMAN—I welcome representatives of the Department of Health and Ageing. We have received your submission, which we have published. Do you have a brief opening statement?

Dr Wooding—I wanted to point out to the committee that we are here in two main capacities. One is information management and information technology policy for the health sector generally. It is important to remember that the Commonwealth Department of Health and Ageing is largely not a service provider. The Commonwealth Rehabilitation Service is the only body providing direct services in any major way. Beyond that, most of the personal and private health and ageing data in the sector is stored elsewhere—in GPs' and doctors' surgeries, in hospitals, in nursing homes and in other such locations. The Commonwealth does fund some services on behalf of identified individuals, mainly through the Health Insurance Commission, which subsidises individuals or service providers for services provided to individuals. We also finance a lot of private and non-government organisations—both not-for-profit and for-profit—to provide services through many other arrangements, such as Aboriginal medical services, nursing homes, hostels and so forth. In that area, our main role in the department is to provide leadership to the sector as a whole as to how it is moving forward with the management of electronic data, attempting to bring more of an electronic and IT flavour into the way health and ageing services are provided, because it is an area which is probably lagging behind much of the economy in its use of IT and its use of advanced information and communications technology.

The other capacity we are here in is, obviously, as an organisation storing and managing personal and private data related to our own activities. Our IT system is under the control of the Business Group, and Dr McLaren and Ms Seittenranta are here to represent our internal IT activity. Mr Sutton and myself are here to talk about our internal information management policies, which include our approach to privacy and confidentiality and the release and use of data.

CHAIRMAN—Does the department issue and maintain a register of Medicare numbers, or is that done by the HIC?

Dr Wooding—HIC issues the numbers.

CHAIRMAN—Do you supervise that?

Dr Wooding—Yes, there is a policy role in relation to policy on Medicare numbers, which is managed within the department.

CHAIRMAN—In addition to the policy role, do you have a role to play in the security of that database?

Dr Wooding—Yes, where we have it in an identified format. The identified data is primarily held by the HIC but, where we might be making use of the data that is provided to us, we have security and privacy policies in relation to that data and the systems in which it is stored.

CHAIRMAN—What I meant was: do you supervise HIC in regard to their security arrangements for that information?

Dr Wooding—Only in terms of the policy leadership role I spoke about. The HIC operates under the various legislative arrangements which are listed at the end of the submission. The HIC has its own board of commissioners and it is a CAC Act agency, so it has its own responsibility for managing information within the HIC.

CHAIRMAN—Your submission talks about the lack of consistency across the Commonwealth, states, territories and the private sector with respect to a national health privacy code. Do you want to talk to that?

Dr Wooding—Yes. The original Commonwealth Privacy Act covered the Commonwealth public sector agencies and established the information privacy principles. Then, at the end of the year before last, we had the implementation of the new private sector amendments to that act, which contain the national privacy principles covering the private sector. But the states and territories have their own arrangements for their own public sectors and some of them—particularly Victoria and the ACT—have also passed legislation which covers the private sector. So some parts of the health sector across Australia are covered by more than one piece of legislation or set of rules—for example, the private sector in the ACT. In other areas we have no legislation—for example, Western Australia and Queensland. What we would like to see is more certainty for everybody working in the health sector, with consistent privacy rules across the sector. Around 300,000 people move state every year. Their health records may or may not move with them and may need to be accessed back in their original state later on. We also have more and more services being provided jointly, with patient experiences across the public and private sectors. So it is essential that everybody working in the system has one consistent set of rules.

Health ministers agreed to this and a couple of years ago established a privacy working group from all jurisdictions. That group has developed the draft National Health Privacy Code and a consultation paper attached to it. Because this is an electronic inquiry, I did not bring copies; instead I direct you to www.health.gov.au/pubs/nhpcode.htm. If you do need paper copies I can get those for you. That document was released in December. We have had public consultations on it in eight states and territories. It is now going to be taken back to the working group for further development, because a lot of interesting issues have been raised in the consultations. What we discovered is that privacy is a very deep and complex area and also a changing area, as practice changes in the health sector. We have taken a lot of views on board. We will be revising the document and then taking it back to ministers in the middle of the year, with a view to what the next steps are. But the aim is to establish one consistent set of rules across the sector.

CHAIRMAN—Some people call for a national individual personal health database held in electronic form. Firstly, what is your view on that? Secondly, if you think that it is probably a good idea, do you believe that you could ensure privacy and be sure that the data could be firewalled from external attack?

Dr Wooding—The answer to the first question is yes, I think that such a system is a good idea. A system of national electronic patient records and a network of national clinical information is a good idea at the individual patient level, where it can be used to improve clinical care—enabling, for example, the avoidance of the dangers of people being prescribed medicines that interact adversely or helping people like anaesthetists understand what people's previous experiences with anaesthetics are. There is a whole range—I could go on for a long time about the benefits at the point of care.

At higher levels there is the ability to research databanks of de-identified data that would help you understand what is happening to the health of the population generally, to help you identify areas where the quality or safety of care could be improved because of the aggregated outcomes in those areas. The health sector will benefit enormously from having that sort of information available instead of as it is at the moment, where it is distributed among silos and is often incomplete and the picture is not very clear.

On the second question of protecting privacy: this system must have the highest levels of privacy built into it if we are going to start to network information in this way. It is beholden upon all in the sector to make sure that the privacy is absolute. You cannot give any absolute guarantees about privacy in the current system or in an electronic system. Privacy is something that we should have very clear legislative and administrative rules around. Secondly, we need to continue to work on systems to improve privacy. Privacy is something you can make better and you can have better quality privacy in the sector. In many ways, the advent of IT improves the opportunity for protecting privacy as much as it provides risks. For example, through IT you can audit much more clearly who has accessed someone's record than you can in a paper based system. So there are some benefits as well. I think we can establish the privacy, but it is definitely one of the key questions on which the success of the whole electronic health project will stand or fall, and we need to get it right.

CHAIRMAN—In your submission, you say that the department is aware of the vulnerability of unencrypted email transmission over the Internet and staff are made aware of proper email procedures. You have not yet isolated yourself from the world where we are all at risk of worms, viruses and all sorts of things.

Dr Wooding—I might have to ask my colleagues to answer that.

Dr McLaren—Our people do have access to FedLink, obviously for exchanging data with other agencies. Other than that, they are required to comply with our policies for Internet usage, and that requires an awareness of the risks and the need to comply with a requirement not to transmit data which is sensitive.

Ms PLIBERSEK—How much do you use FedLink?

Dr McLaren—I do not know the answer to that. It has been available for some time. I think the usage is not that high, but most of the information that our staff exchange with other

agencies is not sensitive and does not require the use of FedLink. But I would have to take that on notice.

Dr Wooding—I think it is important to point out that I cannot think of an instance where we use the Internet to transfer personal or private information. There are other types of confidentiality, such as cabinet-in-confidence or information which is restricted for other reasons, but I think personal and private information is generally not transmitted via the Internet. We are not mainly in that business anyway.

Ms PLIBERSEK—If you did have that sort of information, though, do you mean you would give someone a hard copy of the information, or you would give it to them on a computer disk? How would you normally do it?

Dr Wooding—We have done some transfer of information on protected computer disk delivered by safe hand. We have de-identified information that we download from the HIC over a link. I am not sure of the exact technical nature of that link, but it is de-identified unit record information. We transfer a fair amount of unit record information with fairly high security levels, but it is largely de-identified. Personal information, as a rule, is not transmitted externally over the Internet, although that may change in time as e-commerce becomes more general.

Senator LUNDY—When you say 'security protected', do you use a level of encryption, even for information being transferred across dedicated lines between offices in your department?

Dr McLaren—Within the department, I do not think there is any encrypted information. That is an issue that we need to address. Once again, I think the answer relates to the fact that the information that people generally use in the workplace is not sensitive. An important responsibility of all managers is to manage the systems that they build and maintain in accordance with approved security plans. Security plans for the development of systems, including the storage and exchange of information internally, are developed in consultation with Eija's branch and also with our IT service provider, IBM GSA.

Senator LUNDY—I was predictably going to get to the contractual arrangement you have with IBM GSA and the impact on your security requirements. I do not know whether you heard the previous witness, the ATO, say that their security arrangements are pretty much laid out as service level agreements in the terms of the contract. Is the situation the same with your contract with IBM GSA?

Ms Seittenranta—Yes, it is.

Senator LUNDY—Can I ask the same question about the storage of Commonwealth data assets and whether your contract stipulates that they must be physically held within Australia?

Ms Seittenranta—I would have to take that on notice.

Senator LUNDY—Thank you. Also, I have a couple of questions about data protection and critical infrastructure. You might need to help me here, but I understand that the recent Canberra bushfires did affect some data assets held by someone in the health group of agencies and

departments relating to child immunisation. I understand that some records were destroyed but I am not clear about that.

Dr Wooding—I believe they may have been the ACT government's child immunisation records.

Senator LUNDY—Then I do not need to go down that path anymore. I was not actually sure that I did read something about it. Does that impact on the federal department in any way?

Dr Wooding—The Health Insurance Commission maintains the Australian Childhood Immunisation Register, and I believe there may have been some delays or some problems. Some of that information was required for the immunisation register. If you like, I could take that question on notice and get the Health Insurance Commission to prepare a response for the committee.

Senator LUNDY—Yes. I am interested in the implications, but also the lessons learned, for critical infrastructure protection and data protection—in this case from a natural disaster, a fire storm, but any horrible event in any of your key locations could have a similar impact. That would be helpful. Going back to IBM GSA's role: in the provision of their services do they do applications development for the department?

Ms Seittenranta—No, they do not.

Senator LUNDY—Who does applications development?

Ms Seittenranta—We have an in-house group that does part of it; and, on a project-by-project basis, we may go out to market for people to provide integrated solutions or development work for us.

Senator LUNDY—I appreciate that it is different from different aspects of the health group, so I am probably asking general questions. Mr Chairman, will we be having HIC before us?

CHAIRMAN—I just asked that and have been advised that we will not. But if we want them to come, all we need to do is ask.

Senator LUNDY—It might be worth while following up, because a lot of my questions would relate more directly to them.

CHAIRMAN—We will do it.

Dr Wooding—We may be able to answer some of them if they are general questions about health information.

Senator LUNDY—Going back to Ms Plibersek's point about general security and the way staff are managed, how do you engage departmental staff in privacy and security issues? Do you have a committee structure of employees?

Dr Wooding—I will answer on the privacy and then we will talk about security. With privacy, we have had an information planning and privacy committee. We are currently in the process of moving from that to a different structure, so I cannot tell you exactly what it is. But we have had internal governance arrangements for privacy that have been strong. What we are now establishing is a privacy network, which is a network of officers in all program areas of the department who will be working on privacy issues and developing a level of privacy expertise. We are also working on a handbook, which we will use as a kind of transformational document to improve our privacy processes. As far as we know, there is nothing actually wrong with our privacy protections in the department. We have not had any problems, but process-wise we can do more to make people more aware of it and to make it more understood by all staff. I will have to ask Dr McLaren about security.

Dr McLaren—We see the IT security as a way of providing assurance of privacy—that is one of the reasons why we do it.

Senator LUNDY—Yes, they go hand in hand.

Dr McLaren—We have a security committee, but it is at a much lower level, which manages day-to-day security issues. We also provide some training for our staff. As part of their induction and orientation training and graduate training, all of our staff are given training in security. We also provide ad hoc training services through the department. For example, if people are involved in the budget process, they will get special training and briefing on security before the start of that process. As I mentioned earlier, we also require all systems and databases to have an approved security plan, which is oversighted by the security section and also has audit and fraud control involved. That basically sets out the responsibilities for the sponsor of that system, how they are going to manage the information, the restrictions on the control of it and the requirements for archiving or managing the information when the system or database is decommissioned at a later stage.

Senator LUNDY—My next question relates to assets. Can you clarify whether the IT outsourcing contract with IBM GSA involved the transfer of, in particular, hardware assets to the vendor?

Ms Seittenranta—The hardware, in the main, has been transferred to GSA.

Senator LUNDY—Does that include the mainframe computer for the Health Insurance Commission?

Ms Seittenranta—Can we get back to you on notice on the detail of which ones are with them and which ones are still owned by the department?

Senator LUNDY—Yes. Could you also take on notice for your department—and we will follow up directly with HIC—what your risk assessment is in relation to security, data integrity and data protection by not having the assets in the possession of the department?

Ms Seittenranta—Yes.

CHAIRMAN—Do you have a relationship with the Defence Signals Directorate?

Dr McLaren—Yes, we do. We have a linkage with them. At times they are involved in auditing our systems for security.

CHAIRMAN—So they do that?

Dr McLaren—That is right. I would have to take it on notice to get you the details of our involvement with DSD.

CHAIRMAN—In 2001, you participated in an ANAO audit on Internet security within Commonwealth government agencies. How did you come out of that? It was report No. 13, 2001-02.

Dr McLaren—In the cross-portfolio performance audit of Internet security management we ended up with a quite positive set of findings, in that they found that in general we were adequately managing our information.

CHAIRMAN—Have you had many breaches of security, in terms of either data transfer between your department and another department or breaches of data integrity?

Dr McLaren—I would have to take that on notice. We certainly do monitor. We have ongoing surveillance of data exchanges.

CHAIRMAN—In your submission, you say:

The Department's infrastructure and some services are leased from IBM GSA. IBM GSA are ... obliged to protect ... the data to the same extent that applies to Departmental staff.

Do you audit IBM's performance and, if so, how?

Dr McLaren—Yes, we do audit IBM's performance. Other than our internal audit processes—

Ms Seittenranta—IBM gives us a monthly service report which includes performance on all of the service level criteria including those for security. On top of that there are internal audits and we have had external penetration testing.

CHAIRMAN—You have tested that. You do not just trust them?

Ms Seittenranta—We have had external penetration testing.

CHAIRMAN—And?

Ms Seittenranta—And it has been fine.

Dr McLaren—It has been successful.

Ms Seittenranta—I would have to give you the details on notice which company that did it.

CHAIRMAN—As long as it is fine.

Ms Seittenranta—Yes, it is.

CHAIRMAN—If it is not, we would want to ask why and what you were doing about it.

Dr McLaren—All IBM GSA staff are security cleared like our own staff, so they go through the normal security vetting process as well.

CHAIRMAN—Is that security clearance work up to date?

Dr McLaren—Yes, it is. We run that continuously. All staff and contractors go through the normal security vetting process.

CHAIRMAN—At how many different levels?

Dr McLaren—It depends on the role, but quite a number of the IBM GSA staff are at quite high security levels because of the nature of their work.

CHAIRMAN—Would you mind testing what you have said to me about being up to date on security clearances and come back to us?

Dr McLaren—Yes, we can do that.

Senator LUNDY—Under terms of reference No. 4, there is a paragraph which says:

> Also, the legislation was not written to support the use of health administration data for health service monitoring, quality assessment or surveillance. Restrictions on the use of these data basically limit their use to the management of payments. Recent interest in the uniqueness of these data and the need for information otherwise unavailable has resulted in some linkage and analysis being conducted. However, a more streamlined approval process for Departmental use of these data is needed to fully capitalise on this resource.

The question was the adequacy of the current legislative and guidance framework; so it is really a question about where you think the laws need to change, in the department's view, to maximise presumably de-identified health data for the purposes of policy setting.

Dr Wooding—Goodness me, how long have we got? I think there are a whole lot of issues here. The problem is that the current legislation—the Health Insurance Act, the National Health Act and others—were written in the paper age and they are a bit pre the electronic age. A lot of the rules revolve around keeping databases separate from each other. In an IT environment, that is becoming harder to look at. It is not really a question of keeping them separate from each other; it is having very clear rules on access, clear firewalls and really good technology to protect things. Then there need to be rules where people can bring the data together when they need to. In a way, you might say the old system was based on making data linking hard to do as a protection.

Nowadays we have to go beyond that. We have to 100 per cent protect against data linking where we do not want it to happen, but we need to enable it to happen where it would be useful—particularly in a de-identified form. So we have to work at this. As to whether it actually needs legislative change, a lot of the rules governing the data we have are set by the Privacy Commissioner, most famously under section 135AA of the Health Insurance Act, where

there is a protection against the ways in which NBS and PBS data might be used. That was established in the wake of the Australia Card debate, I think.

It is very important that there is protection on individuals' data being linked together, but this was done a long time ago and IT systems have moved on. As that paragraph says, in looking at the possibilities for analysing data to look at emerging disease trends, changes in service patterns and other things, you are not wanting to look at the identity of the people; you are wanting to look at the patterns of how those people behave. We need to be able to deal with that in a way that still protects individual privacy.

Another issue is around ethical clearance, which is another rather complex arrangement for research involving individuals and often requires a lot of different ethics committees to be brought into the process. It is very cumbersome at the moment and I think we need to think about it, but whether it requires legislative change or administrative change is something we are still looking at.

CHAIRMAN—Thank you very much. Perhaps you would not mind following up with those answers. If we have further questions, you would not mind if we put them in writing rather than ask you back again?

Dr Wooding—No, that is fine.

CHAIRMAN—Thank you very much for coming.

[3.16 p.m.]

BURSTON, Mr John, Chief Information Officer, Department of Employment and Workplace Relations

McMILLAN, Mr Brian Edward, Employment Counsel, Department of Employment and Workplace Relations

O'SULLIVAN, Mr Jeremy, Assistant Secretary, Legal and Risk Branch, Department of Employment and Workplace Relations

PRYDON, Mr Tim, Technical Director, Employment Systems, Department of Employment and Workplace Relations

CHAIRMAN—I welcome representatives of the Department of Employment and Workplace Relations to today's hearing. Thank you very much for coming, gentlemen, and thank you for your submission, which we have published. Do you have a brief opening statement before we proceed to ask questions?

Mr Burston—No, Chairman.

CHAIRMAN—In your submission, you talked about the fact that you monitor access by staff and contracted service providers to your employment systems which hold job seeker records. You say that you regularly check the browse logs to ensure that only authorised access has occurred and that, in addition, where job seekers believe the security of their information has been breached, the department fully investigates all complaints and takes action to ensure that security of the personal information is not compromised. Could you talk to that and tell us whether there is much incidence of it?

Mr Burston—In terms of the technology, we have standard processes in place to do as the submission says; that is, to trawl our audit logs and other things to make sure that those who access the data are entitled to. We believe that that is a pretty sound system, although all these systems are only as good as their first breach, if you like. I am unaware that, since the Job Network has been in place, we have had any significant issues in that area. I am not sure about other members of the panel. I also am unaware as to whether any aggrieved individuals, in regard to data privacy, have ever approached the department.

Mr McMillan—I think there may have been some complaints. Perhaps the easiest thing is if we take that on notice and review the nature of the complaints directly from job seekers and what has been done about that.

CHAIRMAN—You made the issue of it, because you did say:

> The Employment Services Contracts provide for suspension of access of Providers' staff found to be in breach of the Privacy Act. This can, in very serious cases, lead to termination of the contract.

Would you test that for us?

Mr Burston—Yes, we can certainly do that.

CHAIRMAN—To what degree do you use the Internet for information transfer that requires encryption, which you mentioned in dot point 8 in your summary?

Mr Burston—The Job Network arrangements whereby in effect what eight or nine years ago was the CES was replaced by this externalised arrangements subject to competition and so on have been made possible in a technological sense by the Internet. All of our direct dealings—our technical dealings, if you like—between the department as the purchaser and the Job Network members as the providers are done over the Internet. The Internet and Internet access are absolutely fundamental to the operation of the whole Job Network scheme. That interaction is protected by encrypting the data in both directions between the department and the Job Network. Without that technology, the Job Network could not function in the way it has been designed.

CHAIRMAN—I hear you. That being the case, why have you not applied for Gatekeeper accreditation, since significantly you deal with the outside environment?

Mr Burston—There are several issues there. Firstly, in terms of our interaction with the Job Network, our firewalls and technology have been approved and indeed certified by the Defence Signals Directorate so we have the appropriate clearance from the independent technical reviewers on all of this. In terms of Gatekeeper, which gets into another area altogether of public key infrastructure, we are players in the various interdepartmental forums on that but we have not sought to be a certificate issuer or anything like that but we are moving down that path where appropriate.

For example, in the new Job Network round, which starts on 1 July, we are putting in place a situation whereby the use of digital certificates—which is one aspect of the Gatekeeper arrangements—will enable the Job Network members to nominate key individuals in their enterprise to do a lot of what we call the user administration. The function allows the organisation to nominate individuals and how they may access the system. The improved facilities available through what you are calling Gatekeeper we will start using from then.

But the whole matter of digital certificates is very large and very complex. This is an area of technology which is moving very quickly so we have to take an appropriate balance between using the new facilities as they unfold on the one hand but avoiding going too far too fast when the technological ground can move from under you very quickly.

CHAIRMAN—How many different identifiable Job Network providers are under contract?

Mr McMillan—I think we will have 130. I will check that figure. That is the number of entities or organisations that are providing services.

CHAIRMAN—Are they or their employees or both subject to security clearance at any level?

Mr McMillan—Not a security clearance, no.

CHAIRMAN—So they cannot get access to other job providers' files or your information?

Mr Burston—They cannot get access to other job providers' files unless there were a flagrant breach in the system. We certainly have not had one of those yet. When the Job Network members sign up to undertake business on behalf of the government, their staff have to sign standard IT access forms which cover the matters of data privacy, the use of that data and all of that sort of thing so that in effect they function under the same rules or constraints—and certainly the same acknowledgment of responsibilities—that would have applied were those tasks to be directly undertaken by a departmental officer.

CHAIRMAN—Do you audit that compliance?

Mr Burston—Yes. That comes back to where you started. We audit the use of the system in a technological sense and the department also reserves the right to undertake inspections of the Job Network member documentation and processes to ensure that they are complying with the security approach that is underpinning the scheme.

CHAIRMAN—And you have not found any breaches?

Mr Burston—In terms of breaches, we will have to take that on notice. I am not aware of any.

CHAIRMAN—What training do your Job Network providers have to undergo and where do they get it from?

Mr Burston—The department provides a great deal of training on various elements of the scheme on the technology side and also on, what we would call, the business side. We have extensive 'train the trainer' programs for all aspects of the system. For example, for Job Network 3, which starts on 1 July, we have already had 'train the trainer' sessions on that. With respect to the number of people involved, you are looking at, as Brian said, about 130 organisations, which in turn would involve delivery of business out of around 1,000 sites and up to 8,000 or 10,000 individual staff working for Job Network members in various capacities. The only way we can do that effectively is via a 'train the trainer' arrangement. In other words, we make extensive training sessions available to designated individuals in organisations, who then do the training at the lower level.

Ms PLIBERSEK—Mr Burston, I think you said that most of the information that you exchange with Job Network providers is done over the Internet. What system do you use? Do you use FedNet for that?

Mr Burston—We have a variety of technologies. For smaller providers we just use the Internet generally. In much the same way as you may use it if you choose to do your banking over the Internet, we use secure socket layer technology, which you can tell by the little padlock appearing on the bottom of the screen when you interact. In effect, that means that the data is encrypted in each direction. If anybody were to do a print-out—as indeed is typically the case with your bank—they could not find that it was organisation A talking to organisation B about individual 1. They would simply get an incomprehensible data string.

For larger organisations, we narrow that a little bit by using particular Internet links—if you like, a dedicated pipe—but we essentially use the same software in that. There are economies both for the Commonwealth and for the service delivery organisations in that. Let us say, for example, that Mission had 50 sites. Rather than have each of those sites interact with the department completely separately, where the organisations have networks of their own, we can support an arrangement whereby they speak to us through, if you like, one much thicker pipe and then disperse the data to the various sites internally. In that situation as well the encryption technology is in place so that we are able to preserve the confidentiality and privacy of the whole arrangement.

Ms PLIBERSEK—Have you had any problems where people who have worked for Job Network providers have inappropriately accessed the system?

Mr Burston—I cannot speak from the point of view of systems access, but we could take that on notice. There have certainly been instances—and this was in an enhancement that we put over in the last year—where, when someone leaves a Job Network member organisation, particularly when they leave it quickly for whatever reason, we have given the Job Network member the power to cut that access instantly; whereas, in the past, they would have had to fax a form and so on. So, consistent with the approach of devolved administration of all of this stuff, we are pushing that out to the Job Network members where we can. In terms of your general question as to whether any disaffected person has misused the information or behaved inappropriately, we would have to take that on notice.

Ms PLIBERSEK—If I understood you correctly, you said that you have devolved to Job Network providers some of the decisions relating to what level of security authorisation people who work for Job Network might have—what level of access to information.

Mr Burston—Let me explain that. The system is designed around what is best understood as families of access. When we set up the whole system which underpins the contracts we would say that there may be five groupings of tasks, for example, that are legitimate and appropriate in order to carry out your type of business. The department designs all that.

Ms PLIBERSEK—So, if you are doing intensive case management, you will need access to these—

Mr Burston—Yes, you will need more tools than somebody who is not. If you are doing something like elementary job placement, you will need fewer tools. As you can imagine, the more intense the service being provided, the greater the number of tools. We design the tools in a system sense and underpin that with the security access that is appropriate for that function. Once that has been done you cannot have any extra access but it is within your responsibility as an organisation to designate which individuals will have the predefined accesses available. If you identify the person with the authority to make those decisions, instead of a Job Network member faxing many thousands of forms to Canberra—which is literally what happened in the past—for the department to do what is in effect a mechanical task, you can do it under these new devolved security arrangements. That in no way gives anyone access to inappropriate content; it simply says that it is up to you to designate individuals who have the appropriate access for your business so that you can do the final piece rather than send a fax to Canberra to get somebody in Canberra to carry out that mechanical process.

Ms PLIBERSEK—Within a Job Network provider organisation, though, you would have people with a range of different levels of access?

Mr Burston—Yes.

Ms PLIBERSEK—How much do you know about how Job Network providers make decisions about the appropriate level of access for their own staff? Are you confident that they are able to make those sorts of judgments?

Mr Burston—We are, because the whole concept of access is predetermined. It is a bit like going to an auto dealer, in the sense that there might be many thousands of options but in the end you are only offered five or six. We constrain the options. Ultimately, if a Job Network member nominates an individual to do intensive assistance and then gives them inappropriate access for that, it is up to them to sort it out. That can simply be done by human error. But unless that person chooses to be absolutely malevolent—which you cannot screen out—giving the person the wrong access cannot result in any inappropriate updating being made. By doing this, which is our initial step down the Gatekeeper path, we will take a very large bottleneck out of the system.

Ms PLIBERSEK—What do you tell your own staff when you are doing privacy awareness training?

Mr Burston—The ultimate point we make to our people is that information about other people is sacrosanct and is theirs—that stealing information is the same as stealing someone's money. In a practical sense, we make sure that all the data that we use, particularly to test things, is scrambled or processed in such a way that any resemblance to a real individual cannot be derived.

Ms PLIBERSEK—It is purely coincidental.

Mr Burston—Yes, and impossible to trace back. People are very aware of that.

Ms PLIBERSEK—How do you audit the Job Network providers? How do you audit their enforcement of their privacy obligations and make sure that they are doing the right thing?

Mr McMillan—The contract managers or account managers regularly undertake monitoring visits. One of the issues they address in the course of a monitoring visit is the evidence as to observance of privacy requirements. For example, if access to the system needs to be reflected in a document which a staff member signs acknowledging privacy obligations, that would be checked so that we can see evidence that the obligation has been signed for. The principal way of reviewing matters of privacy, in particular, is in the monitoring visits where, as I understand it, privacy is normally on the agenda for review.

Senator LUNDY—Can I go back to the issue of Gatekeeper. You said that you used secure socket layer security. Why would you have to go to Gatekeeper?

Mr Burston—We believe that secure socket layer security is more than adequate for our interacting with the Job Network. Having said that, technologies are changing all the time and

any absolute statement, other than the one I have just made, is not going to last very long. We have used Gatekeeper where we have introduced digital certificates basically to safely devolve a lot of user administration down to the organisations themselves. In the jargon of the day, it is all about 'metasecurity'—it is about simply saying, 'We have got the basic transactions reasonably secured, but now, if we're going to get some of the things that lie behind that—the administrative processes—properly squared away, then Gatekeeper offers us an avenue to do that.' There are other possibilities, but they are only possibilities and we want to look at them very carefully. One of the possibilities for the future that we will look at is whether we would arrange for a digital certificate to be the mode of logging on for every individual for the 8,000 or 10,000 individuals. That opens up a number of other issues—it is complicated stuff—so we think that the sensible way to go is just to get the user administration function sorted out that way. In terms of secure socket layer and other technologies generally, because this moves so quickly, we may be doing it differently in three years, but certainly it is working well at the moment.

Senator LUNDY—Earlier in the day—and I do not expect you to have been listening—we were referring to a government document titled *Australian government use of information and communications technology: a new governance and investment framework* produced by the Management Advisory Committee in relation to IT. It outlines the structure, including an Information Management Strategy Committee and a CIO committee. Is your area involved in those?

Mr Burston—I am on the CIO committee.

Senator LUNDY—Is anyone from your department on the strategy committee?

Mr Burston—No.

Senator LUNDY—Are you involved in any of the working groups of the CIO committee?

Mr Burston—There are six, and the department is on all of them.

Senator LUNDY—This document talks about many things, but it talks a lot about architecture principles and makes the suggestion that:

A federated approach to government ICT governance, architecture and investment is appropriate in the Australian environment.

What does that mean for your department?

Mr Burston—It means that it is better than a monolithic approach, if anyone were to try to set that up. In essence, it is saying that the various agencies—within some commonsense guidelines about interoperability and things like that—are responsible for their own destiny in matters of IT, and really, I think, there is no genuinely workable alternative. We believe that this approach is working quite well.

Senator LUNDY—Could you tell the committee of your status within IT outsourcing and contracting-out arrangements?

Mr Burston—Yes. DEWR IT is provided in house with the exception of one set of facilities competed for back in 1995, which are the touch screens that are available now in Centrelink and Job Network member outlets. They have always been an outsourced provision. The outsourcer is IBM GSA. Other than that, we provide our infrastructure in house.

The only other point to make there is that as with all organisations where there are specialist niches of technology or where there are bursts of requirement that we cannot sensibly fill, particularly temporary ones through traditional Public Service arrangements, then, of course, we are relying on IT contractors. In the jargon, I believe that is now referred to as contracting in rather than contracting out. We are not in a large-scale outsourcing arrangement.

Senator LUNDY—I have a general question in relation to metadata and archival integrity: how advanced are you as a department in solving those issues?

Mr Burston—One of the things we have learnt about things like that is that the issues are too important to try to do them totally by yourself. Under the CIO council arrangement that NOIE is running, you are seeing working parties into five or six heads of issue and I think at least one of the ones you mentioned is there. We have to work out a sensible middle ground between agency autonomy on the one hand, keeping up with the technical flexibility on the other and yet moving ahead. That is essentially what we are doing.

Senator LUNDY—What do you see as the benefit of the CIO committee in this framework and how it relates back to your ability as a department to provide a secure environment in IT?

Mr Burston—The main benefit so far has been the sharing of information. It is a bit daunting to sit around a table with, in the order of, 30 CIOs and realise just how diverse and large the Commonwealth is. You have people from the Defence Signals Directorate who are very interested in security, particularly national security. On the other end of the spectrum, you have people such as our predecessors at the table who are interested in very light and flexible ways for the delivery of things like pharmaceutical benefits. You have the ATO whose charter it is to safeguard the revenue and whose IT systems reflect that approach. You have people like ourselves who, by virtue of the government arrangements with the Job Network, have to be very flexible and able to move very quickly.

When you get around the table and you share a great deal of information, you see that, despite what are in some ways the surface dissimilarities, the underlying issues stay the same: interconnectivity; time to market; movements in technology generally; how best to handle disruptive technologies—all of those things, to which there is no simple answer. We have certainly found that the more we share information with our colleagues, the better the approaches we take.

Senator LUNDY—As you have responded to growing awareness about the appropriate IT related issues that are, in fact, whole of government—such as standards, security, privacy et cetera—how well resourced is your department in responding to those changes?

Mr Burston—The classic one that we will talk about is interoperability. No department is sufficiently resourced, given their onerous day-to-day service delivery responsibilities—or in the case of the central departments, their policy responsibilities—to take on all of these issues. What NOIE has come up with, which I think is working quite well, is the concept of a lead

agency. In a lot of those working parties, they will say, 'No-one is going to have the money to do all this by themselves, but so and so may, given the nature of their responsibilities, be a bit further down the track than others. So we will make them the lead agency and then we will have a working party to get the best thinking from the various areas and see if they can work out a way ahead.'

There is a particular challenge now which the CIO council—and I assume ultimately the IMSC—will have to come to grips with it, and that is this whole concept of joined up government. The Internet provides, at the front door, portal technologies and things like that which in theory, to take an example, mean that, if you want to set up a small business, the technology—if the rest of the world can organise itself well enough—would enable a small business person to be presented with the 56 places, or whatever is the amazing number that they have got to have to start a business. At the moment, as you know, they go forum shopping and they jump over one loop and then they find, 'Goodness me, we are on this plateau. There are these seven sets of bureaucrats that we have to placate and then there is this over here.' The technology is coming to the point where, if we can organise ourselves well enough, we can integrate a lot of that. But there are some very big issues in that. I think the CIO council provides a forum for us to start working through some of that.

Senator LUNDY—On your hardware—on your systems—do you host anyone else's data or provide services?

Mr Burston—By virtue of machinery of government changes, the employment department was, as you may be aware, up until the end of 1998 with education in a department called DEETYA. Then the employment part joined workplace relations. The net effect of that was we continued to provide the technology platforms for education up until November last year. They are gradually taking on some of those themselves now. The reason why we are able to do that is that we had a nice integrated system in the former department so it made sense for them to source their platforms from us.

Senator LUNDY—When you say that you mean you had two big mainframes?

Mr Burston—No. The mainframes are easy because they are few and it is solved technology. The real issues are the mid range and the desktop, where the possibilities for divergence are limited only by the imagination of some of the technologists.

Ms PLIBERSEK—I thought you were going to say 'of the purchasing officers'.

Mr Burston—In my experience, I have never found a purchasing officer with imagination.

CHAIRMAN—I have had some that have had unbelievable imagination.

Senator LUNDY—Just to clarify, who has the mainframes that service the education department—you or education?

Mr Burston—About a year ago, as part of working it through—there may have even only been two—there is now no mainframe looking after that. Basically, they redeveloped their systems onto what they call the mid range, which is the smaller range of servers. We now have one system left on the mainframe, which is the one that drives the back end of the Job Network.

That is because of the scale of that. We look after them but we are now doing progressively less for them as they have taken over their server layer and their desktop. We still provide the communications framework for them. But as well as that, by virtue of the last machinery of government change—the one in 2001—we provide the platform for the business entry point.

Senator LUNDY—Still?

Mr Burston—Yes. It is now done out of the industry department.

Senator LUNDY—I was going to not ask any questions about that because I though it had gone.

Mr Burston—All I know in terms of the business entry point is we provide the hardware platform—the pure technology layer. The business issues, fortunately, are now with the industry department.

Senator LUNDY—Finally, what software platform and operating systems do you use?

Mr Burston—We have an IBM compatible mainframe, so we have the IBM MVS system. For the desktop, we have Windows 2000 XP. For the server range, we have Windows 2000. For the network operating system, we also have Windows 2000.

Senator LUNDY—That should do me. I was going to ask you about patches and if you have had any problems in getting patches in time to resolve issues.

Mr Burston—In terms of patches for operating systems, in general it is not too bad but there can be an undignified flurry every so often when we find viruses or something like that, which in turn—occasionally; not always—can be traced back to defects in operating systems. Moving to new versions and so on can be a challenge. Typically, the challenge is not in getting the new version from the provider—in this case Microsoft. That can be relatively easy to do. But you have the problem of the various applications—the various systems—sitting on the earlier version. Instantly switching over is not always as quick as we would like.

CHAIRMAN—The last question is that in 2001 the department undertook an AO performance audit of Internet security within Commonwealth government agencies. Can you tell us how you fared?

Mr Burston—I cannot recall.

Senator LUNDY—You were one of 10 departments.

Mr Burston—We certainly were one of 10. I cannot recall whether any of the recommendations out of it caused us particular pain. I am not sure—to use the vernacular—whether we were pinged anywhere. If it had been bad, I am sure I would not have been allowed to forget it. I think in general we emerged from that pretty well.

CHAIRMAN—Is it the wish of the committee that additional exhibits 3, 4 and 5 today—from the ANAO, *ANAO audits in ANAO's submission to the JCPAA* and *Internet delivery*

decisions: a government program manager's guide, and a folder of additional information from Centrelink—be accepted as evidence and authorised for publication? There being no objection, it is so ordered. I thank participants in the hearing, our colleagues, JCPAA staff and, most importantly, Hansard.

Resolved (on motion by **Ms Plibersek**):

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

Committee adjourned at 3.51 p.m.