COMMONWEALTH OF AUSTRALIA

Official Committee Hansard

JOINT COMMITTEE OF PUBLIC ACCOUNTS AND AUDIT

Reference: Management and integrity of electronic information in the Commonwealth

MONDAY, 16 JUNE 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, 16 June 2003

Members: Mr Charles *(Chairman)*, Ms Plibersek *(Vice-Chair)*, 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 Humphries and Senator Lundy and Mr Charles, Mr Cobb, Mr King 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 11.08 a.m.

CHAIRMAN—The Joint Committee of Public Accounts and Audit will now continue 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 fifth public hearing for this inquiry. Today we will hear evidence from two important entities, one from the public sector and one from private enterprise. Evidence will be given by the Defence Signals Directorate and Microsoft.

Before commencing proceedings, I advise witnesses that the hearings today are legal proceedings of the parliament and warrant the same respect as proceedings of the House itself. The giving of false or misleading evidence is a serious matter and may be regarded as a contempt of parliament. The evidence given today will be recorded by Hansard and will attract parliamentary privilege. Finally, I refer any members of the press who are present to the committee's statement about the broadcasting of proceedings. In particular, I draw the media's attention to the need to report fairly and accurately proceedings of the committee. Copies of the committee's statement are available from the secretariat staff.

[11.10 a.m.]

BLACK, Mr Allan Louis, Manager, Government IT Security, Defence Signals Directorate

BURMEISTER, Mr Tim, Acting Assistant Secretary, Information Security, Defence Signals Directorate

CONNICK, Ms Lynwen, Assistant Secretary, Information Security, Defence Signals Directorate

MERCHANT, Mr Stephen, Director, Defence Signals Directorate

SCOTTON, Mr Michael Robert, Manager, Industry Liaison, Information Security Group, Defence Signals Directorate

CHAIRMAN—I now welcome representatives of the Defence Signals Directorate to today's hearing. We have not received a submission from you, but as all who are here know, you gave us a very valuable private briefing on these issues earlier this year. Would you have a brief opening statement for the public record?

Mr Merchant—I do. I hope that our earlier appearance and the opportunity to demonstrate some of the potential vulnerabilities have been helpful to the committee in its subsequent sessions.

CHAIRMAN—Could I emphasise the word 'brief'.

Mr Merchant—Sure. First of all, we welcome the opportunity to appear before the committee today. It is an important issue, although one that does not always attract the public profile that perhaps it warrants. Information security is core business for the Defence Signals Directorate. It sits alongside the collection and reporting of intelligence from foreign signals as one of our two main business lines in the directorate. Those functions, as members of the committee would appreciate, are really two sides of the one coin for us. Certainly the tools, techniques and skills we develop in our signals intelligence function give us great insights into what we need to do and, indeed, other agencies need to do to protect their information.

I also make the point that the two functions employ people with very similar skill sets. So having those two functions housed in the one organisation I think allows us to recruit, train and develop a pretty robust base of talent in which we are able to feed both of those business lines. Certainly, I think that makes it easier to feed the appropriate skill sets into the information security function than if information security somehow sat outside DSD.

The other point I would like to mention very briefly in terms of context is that, of course, even though the Defence Signals Directorate is a part of the Defence portfolio and I report to the Minister for Defence, in both signals intelligence and information security, we fulfil a national role for the Australian government. We are the national authority for information security. We are also the national authority for cryptology as well as the national foreign signals intelligence

agency. While Defence is a really important customer for us regarding the products of both of our business lines, we are very conscious of the need to service all of the Australian government agencies, particularly in the information security function. We try very hard at least to meet all of their priority requirements, obviously, within finite resources.

I will finish by saying that our information security function in DSD has changed a great deal in the last 10 to 15 years. With it, the approach that we take to this line of our business has changed as well. Our original focus in information security—we have been in this for a long time, 57 years or so now for the directorate—was very much on the security of Australian government and defence communications systems that carry very highly classified national security information. That remains a very important part of our information security role. In fact, of the 80 or so people we have employed in information security functions, about a quarter of them are still devoted to that effort. We are unapologetically obsessive, strict, controlling and policing. As our information security agenda has broadened to get into areas of e-security and protection of the national information infrastructure, we realise that that approach is not always appropriate. We are still very strict in some aspects of that work, particularly when it gets into the accreditation of products. However, increasingly our relationship with other government agencies is one of partnering, collaboration, education and advising on appropriate risk management. As I said earlier, our approach was unapologetically risk averse, but as the agenda has broadened, we have realised that both our philosophy and the risk management approach need to change.

I hope that has been useful in giving a bit of an overview of and context for where DSD sits in this. We have a number of documents here which we would be pleased to provide to the committee. One is a compendium of formal DSD publications relating to information security. We have a pamphlet on our incident security reporting scheme and a ready reckoner on the same issue. They are part of our customer relations products.

CHAIRMAN—Thank you very much.

Senator LUNDY—I move that they be received as evidence.

CHAIRMAN—There being no objection, it is so ordered. Most people seem to love you, but you have your detractors. I do not know whether you have read transcripts of our evidence. Optus said:

> The whole DSD accreditation process around secure Internet gateway facilities has also created a huge problem for the Commonwealth because there are only two secure gateways through which they can get out to the Internet: SecureNet and 90East. The process of obtaining that accreditation is enormously expensive.

Would you like to comment on that.

Mr Merchant—I might make some introductory comments and then hand over to some of my colleagues. Lynwen might like to add to this. It is an expensive process—we acknowledge that—but as I said in my opening comments, that is one area of our work where we still apply very strict standards. The standards that we apply in our evaluation process are internationally recognised standards. They are not standards that DSD influences on its own. We could

compromise on those standards, but that would impact on the mutual recognition of products that we evaluate. It would also impact on the security implications.

What we are interested in doing is evaluating products to ensure that they are fit for purpose. When those products involve ensuring the security of connections between government systems and the Internet, they need to be of a very high standard. A lot of our evaluation work is now done outside DSD in commercially registered facilities run by private companies. We do not control the cost charges.

That is based on a commercial activity. Where DSD needs to certify the work that is being done, we do that on a cost recovery basis. Depending on the level of evaluation that is being sought, our costs range from about $5,000 to $30,000 for the DSD component of that. We generally waive that cost where there is a Commonwealth government sponsor for the product being evaluated. From DSD's perspective, the regime—and we have looked at this—is justified in terms of both the standards and costs associated with it. Lynwen might like to add to that.

Ms Connick—I guess there are two components to gateway certification. There are public companies who have gateways certified and then sell services on to government agencies to use those gateways. But there are also government agencies who might have their own gateway to the Internet certified. DSD performs services to both those two customer sets.

In terms of how expensive it is, it depends on the security infrastructure the organisation already has in place. Organisations that have very good security practices and facilities find that it is not a very expensive process. The DSD component, if we do cost recovery, is fairly cheap in comparison to services that they buy from private sector providers. But organisations that do not have a security infrastructure in place might find they have to develop new practices and new physical security infrastructure to get certification. That component might be a bit more expensive for them. So different organisations find it different.

In terms of the number of gateways available, there is no limit. Any company that wants to can set up as a public gateway provider. I guess market forces determine how many there will be. But certainly if agencies want to provide their own independent gateway, they can do that as well. So there is really no limit there. Allan might have more details on the gateways we have certified.

Mr Black—In fact, there are three commercial service providers, not two. What we do not have any visibility of is how many agencies are contracted—

CHAIRMAN—Two secure gateways?

Mr Black—No. There are actually three.

Senator LUNDY—What is the other one?

Mr Black—There is 90East, SecureNet, and CSC provides the third gateway service for Commonwealth government agencies.

Mr KING—They do our offices, don't they, CSC?

Mr Black—I am not sure. There is a lot of infrastructure that has to go—

CHAIRMAN—In fact, Optus complained about that. They said that they can virtually charge monopoly prices because there are only three competitors. Optus is a competitor of theirs, so they have all the intellectual property.

Mr Black—I do not know what the costing regime is that the gateway service providers offer. They actually offer more than just the Internet gateway because there is a whole lot of infrastructure behind the gateway itself. I suspect that that is where a lot of the cost is incurred—in setting that infrastructure up to provide intra-agency communications as well. I do not know the exact numbers of agencies that have their own gateways, but there are a number of agencies that provide their own secure Internet gateway rather than go to an outsourced function.

Mr Burmeister—About 15.

Ms Connick—We hope that if people find it costs too much, there is a market opportunity for someone else to become a gateway service provider. That is the way it should work.

CHAIRMAN—I think I remember from our private discussions that we had some discussion about open source versus closed source. Would you like to tell us about that again. There is a commercial interest out there, and it has generated some controversy as the hearings have progressed.

Mr Merchant—And the issue is the evaluation of open source.

Ms Connick—There are advantages and disadvantages to open source and closed source software. The advantage, I guess, with open source software is that everyone can see the source code, they know a lot about the product and it gets a lot of visibility. The disadvantage is that it often changes frequently. There is often no particular supplier who is willing to put that product into an evaluation. It is usually particular vendor products that get evaluated. We would certainly recommend that products should be evaluated so that you know they are doing what you think they are doing. That is why we run an evaluation scheme. There is no reason that someone could not decide to put an open source product into an evaluation. It is just that someone has to decide to do that. I understand that there are people in the US who are looking at doing that and getting some open source products evaluated through an evaluation scheme similar to the one we run under the AISEP program here in Australia. So I guess we have an open mind about open source software. We do not—

CHAIRMAN—An open mind about open source software. Could we quote you on that?

Ms Connick—We would be happy to look at it if someone wanted to get a product evaluated. We do not recommend using security products or encryption products that have not been scrutinised or evaluated. Even though they are open source, that does not necessarily mean that people have been able to look at all the vulnerabilities. These sorts of products have lots and lots of lines of code. It is a very difficult process. Just because the source code might be open does not mean that someone has been through a rigorous evaluation process.

Ms PLIBERSEK—Can you tell us a bit about the ISIDRAS reporting arrangements and what sort of information you are gathering?

Mr Merchant—Sure. I will make some opening comments. Others might like to then elaborate. Basically, the ISIDRAS reporting scheme, from our perspective, is working quite well for us. There are four levels of incident. The top two are actually mandatory to report. I know when we appeared previously that there was some discussion about whether all incidents should be mandatory to report. We have discussed that further since the earlier appearance. It is very much the view of the people in our network vulnerability team that if you move to a mandatory reporting regime for all levels of incidents we would be swamped with information which would not really give us any additional insights. Certainly the amount of information we now have from the ISIDRAS reporting scheme gives us a good understanding of what is going on out there and enables us to provide appropriate value adding advice for the higher level incidents.

Ms PLIBERSEK—I am interested in you telling us about what is out there. I would like you to tell us about that.

Mr Burmeister—I will go through the various categories within the scheme itself. Category 1 basically are events which are anomalous but nobody can really determine what they are and they have no real effect on information security. Category 2 is a slight increase on that. Again, it has no effect on system operations or no compromise is identified, but an unsuccessful attempt to actively breach has occurred. Categories 3 and 4 are obviously situations where a breach has occurred and a compromise is likely.

We are currently getting some voluntary reporting on category 2 incidents which typically are things like port scans. They involve people knocking on the security door to see whether there are any openings. We do that with a number of agencies. The sort of reporting that we would see would be in the order of hundreds a week regarding those sorts of events. That typically is the background noise you would see on the Internet. If you had a firewall, for example, on your own desktop system in the office, you would see those sorts of doorknocks appearing on your own systems, depending on how your firewall is set up.

Categories 3 and 4 in practice are relatively small in number in terms of the overall amount of noise there is. They typically will be things like web site defacements, where somebody has actively got into a system and has been able to do some damage, all the way through to the ones that perhaps we would not pick up, which are very sophisticated attacks that may not register on any of the defensive systems that people have in place. Essentially, DSD is really interested in that latter group of activities. ISIDRAS itself does not help us pick that up. We have all sorts of other sources that we use in our work to try to develop systems that will pick those sorts of things up from a national security perspective. Category 3 and 4 incidents reported to us give us an overview of the level of sophistication of attacks that people will experience over the public network. They set a baseline, I suppose you could say, that we can work with to understand what further information we need to seek to try to find more sophisticated attacks that nobody at the moment can identify. Does that answer your question?

Ms PLIBERSEK—We had some evidence from the CSIRO that they were not reporting because of the frequency of reporting expectations. They find it impractical because they get

maybe millions of sweeps a week or a month. Can you tell us a bit about the CSIRO and what your view is of their criticisms of the system?

Mr Burmeister—They would be referring to what we consider category 2 items. We would not be expecting them to report those to us. Where they actually have definite breaches of their security, we would expect it. Over the years the program has been running, I am not sure the CSIRO has ever had a reportable incident. One of the problems with ISIDRAS, obviously, is that the mandatory reporting scheme has the same problem that most reporting schemes do; we need to make it a visible scheme. We are taking steps to do that with our pamphlet, ready reckoner and information sessions. So there has been in the past probably a vacuum, I guess, where people have not understood that the scheme has existed. It is also a scheme that, in the past, there was no real response, so people reported but nothing really came out of the scheme to say there was any benefit in it. We are now providing a response capability to agencies. If they do have a problem and report it to us, we can help them fix the problem, identify it and make sure that it does not happen again for them. So there are now people at the end of the line who will be able to work with them to fix any problems they identify.

Ms PLIBERSEK—Could you give us an idea of how many level 3 and 4 incidents there would be in a week, say?

Mr Burmeister—In a week, we would be lucky if we got one or two. We would expect probably about 40 or so incidents a year. That is in terms of—

Ms PLIBERSEK—Of 3 and 4 together?

Mr Burmeister—Of 3 and 4 together. That is in terms of the current understanding of ISIDRAS as a scheme. We would anticipate that, as ISIDRAS itself becomes more widely known and people understand that there is a resource behind it available to them to deal with incidents, the reporting becomes a bit greater. We might see that go up a bit more. But we would not see it as a very large percentage of the overall number of incidents that people see.

Ms PLIBERSEK—When you talk about having the capability of responding and helping people if a breach has been attempted or whatever, do you then contact other agencies that might be vulnerable and warn them of the problem?

Mr Burmeister—Yes, we do. If there is what looks to be a common issue, we would put out our own advisory, but we very rarely do that. If there is an incident breach, there is usually some sort of reason for it and there is usually some sort of advisory about a vulnerability that has been issued that deals with it. We very rarely see something that is unique. We would just go out to our constituents and remind them that there are vulnerability issues and there are relevant advisories from groups like AusCERT, for example, that deal with a particular issue. If there is a trend in people not patching for a particular vulnerability, we will put out an advisory that highlights that issue for everybody.

Ms PLIBERSEK—How many advisories would you need to put out each year?

Mr Burmeister—So far this year we have put out one. Last year we put out about seven. We would not expect to put out more than about 10 a year. Our view would be that less is better.

There are a number of organisations putting out advisories on vulnerabilities and we do not want to duplicate their work. We are interested in things we can evaluate.

Mr KING—I want to understand the appropriations with the budget. Does it come through the defence department?

Mr Merchant—Yes, it comes through the defence department. Funding for DSD is part of the Defence portfolio.

Mr KING—That is the reason for your name, is it? It seems to me that your brief is much broader than just simply defence.

Mr Merchant—It is. We could go into the historical reasons why DSD is part of the Defence portfolio. Not least of all, as I said at the outset, one of those is because Defence is such a big customer of our products. Yes, all of our funding comes from the Defence portfolio. We are basically a line item in the Defence budget.

Mr KING—You mentioned earlier that you had an informative booklet that you may be prepared to distribute.

Mr Merchant—Yes, we have all of these here.

Mr KING—I will have to go. I was wondering whether I could have one. Thank you. Finally, I wanted to say I thought your response to the Optus comments was very appropriate. The perception I have as a newcomer to this process is that you have a very secure and appropriate system of surveillance in place that is not too intrusive but on the other hand is sufficiently broad in its coverage to have that level of security, which I think is very important.

Mr Merchant—That is the balance that we strive for. As I have said, we come from a background—it was the point I was making, too—that was very strict and risk averse, but we are conscious that that is not the approach that is now appropriate in a uniform application across all areas of our information security work. But there are areas where it still is appropriate. We try to identify them fairly precisely and limit that type of approach to where it is necessary. In the broader range of our functions, we have an approach that is based more on risk management, advisory and education rather than a risk averse policing type function. I think some of our reputation, which I am pleased to hear from the agencies you have spoken to, is fairly positive. But with respect to those who have a bit of a negative view of DSD, some of it still flows from a bit of the history and origins of our work in this field.

Senator LUNDY—I want to follow up on the issue of how DSD reports to the executive. Apart from obviously receiving the resources through the Defence budget and being a line item in the budget, how do you report back to the members of the executive government for your whole-of-government role on NOIE and e-security matters?

Mr Merchant—There are a variety of ways we do that. Clearly, in all of our functions we are accountable through the secretary's committee on national security to the National Security Committee of cabinet. That covers both our signals intelligence and our information security functions. Clearly, in a lot of our information security work we have picked up in recent years,

we have been part of a whole-of-government initiative where we have participated with other agencies such as NOIE and ASIO. Those submissions tend to go through the same process of the secretary's committee on national security through to the NSC and then through our annual reporting mechanisms. Lynwen, do you want to add anything to that?

Ms Connick—I guess we provide information to people like Attorney-General's and ASIO when they are reporting on security aspects. Attorney-General's run the protective security policy committee that provides reports on the security of government agencies. We provide information to them that we have come across during our work as well. So there are a number of different agency reports that we contribute to as well as our own annual reporting.

Senator LUNDY—So with Attorney-General's, as far as protective security goes, what about the cryptography role DSD has?

Ms Connick—That is already included in that.

Senator LUNDY—Through the secretary's committee on national security?

Mr Merchant—To the National Security Committee of cabinet.

Senator LUNDY—I turn to the issues Optus raised. I want to clarify the secure gateway status and the fact that there are three private companies and some 15 agencies and departments with a secure gateway. Optus made the point in our hearing with them that the standards for what constitutes a secure gateway do not distinguish between the Internet and a virtual private network, or VPN, or indeed a private network. Can you clarify for me whether Optus are correct in saying that and the status of physical private networks like Fedlink in the midst of that? I think Fedlink is a VPN. What is the difference? Have Optus got a point?

Ms Connick—Broadly, the requirement is that people use, in particular, evaluated products when they are connecting a classified government network to a public network. We do not distinguish between the Internet and any other public network. So we have a requirement there if there is a connection to a public network, which is usually the Internet. There are not really any others around at the moment that use evaluated products. In general, people will seek to have a certified gateway to do that. Fedlink, I guess, is a different issue. Fedlink has a different certification process when agencies connect up to Fedlink. It depends on the level of the network.

Senator LUNDY—Fedlink is a VPN, isn't it?

Ms Connick—I guess it is.

Senator LUNDY—Does it have the same standards as the secure gateway requirements?

Ms Connick—In general, people will have a gateway certification to connect to Fedlink. There is a set of requirements for connecting to Fedlink depending on the classification level of the network connecting. So there are different classification levels and confidence protection that can be connected and there are different requirements depending on what agency is connecting

through Fedlink. DSD provides services at particular levels, and agencies can do their own certification at the lower levels.

Senator LUNDY—So Fedlink is, for the purposes of your standards, an open network, a public network?

Ms Connick—Fedlink goes over public networks, yes.

Senator LUNDY—It seems to me that Optus is arguing they could provide Fedlink as a commercial entity as opposed to a government entity?

Ms Connick—Fedlink is operated commercially. There is a limit to how many different commercial solutions we want.

Senator LUNDY—That is the point. Fedlink seems to have a different status from other commercial products like those Optus are suggesting and obviously a different evaluation process and different conditions through which agencies can evaluate.

Ms Connick—NOIE would be best placed to talk about the detail of Fedlink. As I understand it, a tender went out for people who wanted to provide a Fedlink type service. One supplier won that tender. It was an open process. A number of different people, including Optus, could compete for it. There is a limit to the number of different secure networks you can accommodate when you want government agencies to be able to talk to each other. On the one hand, you want a competitive process, but you cannot have a number of different networks that will not talk to each other. Allan might be able to say something on Fedlink.

Mr Black—There is a little difference. Optus were referring to their product OPI Trust. OPI Trust uses a product that was evaluated under the Australasian information security evaluation program. But it is only one part of the total service they provide. We do not have any assurance over that total service. We can certainly comment on the evaluated product, because we did that, and say, 'Yes, there is a level of trust in that.' But it is the broader service.

Fedlink, from agency entrance to agency entrance, uses a DSD evaluated product that is a Cisco IP router. We know the trust. Even though it is transiting across the Internet, there is confidentiality provided from agency to agency. Sitting behind that again is an evaluated gateway, either self-regulated by the agency, if it is up to the in-confidence level, or DSD if it is to the protected level. So there is a slight difference. We have looked at Fedlink and determined that the architecture is suitable and that it is fit for purpose.

Senator LUNDY—I am interested in comparing Fedlink with the Optus part. What was the Optus part name?

Mr Black—OPI Trust.

Senator LUNDY—What elements of that product are not part of the picture you can see?

Mr Black—I do not know the exact product name. I believe it is to do with part of the provision of the authentication within that trust. As I was saying, it is part of the broader Optus

network or the Optus service that is provided under OPI Trust. What we do not know and have any visibility of is what is happening to the Commonwealth data when it is in that network.

Senator LUNDY—But do you with Fedlink at a protected level? I would say not.

Mr Black—We have a level of trust. From agency to agency, the confidentiality of the Commonwealth information is assured.

Senator LUNDY—It is a level of encryption?

Mr Black—It is the level of encryption that will provide the level of trust in protecting Commonwealth information while it is transiting across the Internet, yes.

Senator LUNDY—While it is out there?

Mr Black—Yes.

Senator LUNDY—With Optus's product, it is the level of encryption, because you do not know what is happening to it when it is out there?

Mr Black—We do not know what is happening with the Commonwealth information while it is in the Optus network in the OPI Trust. We do not know at what stage it is encrypted and at what stage it is unencrypted.

Senator LUNDY—It is very unclear to me. Optus were making a clear point, but it was unclear to me, given what I knew about Fedlink, what the relationship was between the two and why, if Fedlink could be installed or evaluated up to the protected level, their product could not. It had to come down to, I presume, the technical specifications of it.

Mr Burmeister—It is actually the facility within which they run the product. So the product itself has trust until it reaches that facility.

Senator LUNDY—What do you mean by 'facility'?

Mr Burmeister—Whatever environment Optus is providing to run that particular product in. It must connect to other things so that it can move traffic around. Really we are saying that while we have evaluated the product itself, we have not evaluated the facility that Optus intends to provide and through which it is going to shunt traffic, whether it goes from one OPI Trust product into another. At some stage in the facility, it is going to handle the data in some sort of clear form, probably.

CHAIRMAN—Is that because they consider it proprietary information? They do not want you to know about it?

Mr Burmeister—When we talk about gateway certifications and Fedlink certifications, we are really talking about the way the connections are made at every stage. So if it leaves a trusted environment A to move into a trusted environment B, what is the level of trust in that environment between the two of them? In the secure gateways, as I understand, we have a level

of trust around the whole facility. We know where the data is going. We know how it is being handled and who has access to it. That is really the process of certification, as I understand it. As I can understand it, the difficulty Optus has is the amount of money it would take them to develop a secure facility, using what they believe already is an evaluated product, to provide the level of assurance so that we in DSD would then be able to certify that the facility itself, not the product, that handles the data after that is up to our required security standards, which we are asking everybody to adhere to. It is a commercial issue for them, really.

Ms Connick—No-one has asked us. There has never been a government agency that has come and asked us to look at it because they want to use it. So we do not generally get involved in going out and looking at various products and facilities unless we have been asked to.

Senator LUNDY—You have anticipated my next question well. What opportunity is there within your current structures for approval or evaluating to actually make that assessment and perhaps give Optus this type of advice? Is there a system or a process in existence when a competitor is knocking at the door, so to speak, but is unable to get the next step because of some sort of technical issue about their facility? At what point is there an obligation on DSD to take that step to in turn facilitate competition?

Ms Connick—That is probably something that would be best asked of NOIE, because they are the ones who set up Fedlink as a whole-of-government secure facility to access the Internet.

Senator LUNDY—I appreciate that. Do you think NOIE and Fedlink are getting special treatment?

Mr Merchant—Fedlink gets special treatment because we have a specific role in providing technical advice to NOIE about the standards that need to apply within Fedlink. NOIE has been through all the previous processes to set Fedlink up. Our role is to ensure that it is fit for purpose, if you like—the components of it. Optus is quite free to come to us, or we to go to Optus, but more likely they would come to us, to talk to us if they wanted to explore the option that Tim Burmeister was talking about of how they would get accreditation for the totality, if you like, of what they would see as an acceptable alternative, which is what I understand they are arguing. Indeed, they have spoken to us about that issue. It is not as though we have been putting up barriers and saying, 'No, you're not in this.' We don't operate that way.

Senator LUNDY—I certainly understand that. It then becomes an issue of at what point DSD were brought into the process of evaluating Fedlink if you were involved in the design of the Fedlink system. I think it is a very important question, not necessarily of DSD, which is the point that was made by Ms Connick. At what point is it appropriate for the government to create an equal playing field for other possible providers of that service? I think that was the key point Optus was making.

Mr Black—I met with representatives from Optus last year when they were considering marketing—I cannot remember the exact stage of their decision—OPI Trust. This very question came up: can Commonwealth government agencies use this product, OPI Trust? At that stage they described the architecture and the concept they were going to provide. At that point I identified to them things that needed to be addressed. Regardless of whether we decide that it is suitable or not suitable, a Commonwealth government agency could choose to use OPI Trust

provided that they were satisfied with the regime in place to protect Commonwealth information because, according to the PSM, the agency has that responsibility. We would sit down with the agency, if that is the service they were going to buy, and work out the best way to ensure that Commonwealth government agencies' information is secure. So we did sit down very early on. In fact, there was another carrier we sat down with before Optus who were considering doing a similar service. They chose not to enter into that market at that stage. We did sit down with Optus to try to work out the things that had to be addressed in terms of ensuring the protection of Commonwealth information.

Senator LUNDY—The next issue relates to the market and market access by commercial operators. There is the issue of those who are able to perform evaluations on security products. My understanding is that it is Tenix, Logica CMG and CSC. Are there any others?

Mr Scotton—There are not currently any others. From 1 July, we are opening up the licence regime to allow any qualified evaluation facilities to participate.

Senator LUNDY—How do you manage that evaluation process effectively? What is your relationship with these companies who are accredited to perform evaluations? How do you manage that process?

Mr Scotton—We play the role of the certification body, which means that the actual product evaluations are conducted by the commercial facilities. The role we play is partly oversight in that we check the technical correctness of their procedures and make sure that the conclusions they reach are reasonable. That involves an ongoing level of interaction with the labs. We are also responsible for making sure that they maintain their technical standards. We also do that with NATA, who have a requirement to check their accreditation once every year.

Senator LUNDY—The obvious point there is that CSC, who also are a secure gateway provider, are also evaluation accredited. I presume by that that they would be assessing companies that could be competing against them in certain circumstances. How do you manage the perception that a conflict of interest could develop?

Mr Scotton—Licensing agreements have quite a lot of detail on potential conflict of interest. An important aspect in setting up an evaluation facility is to ensure that it is actually a separate line of business from the rest of the organisation, so it needs its own separate facilities and own administrative support. If they consider that there is a conflict of interest arising, they need to discuss that with us. That is part of our oversight responsibility.

Senator LUNDY—Have they ever done that?

Mr Scotton—Not to my knowledge.

Ms Connick—Not that I am aware either.

Senator LUNDY—In terms of that process of evaluation, can you take me through what it involves in a physical sense and particularly whether or not it is all done here in Australia.

Mr Scotton—We assess information security products against an international set of criteria known as the common criteria. That is a way of expressing particular security functionality for a product. When a vendor wants to have a product evaluated, they need to develop what we call a security target. The security target is specifically the security functions that they are claiming the product provides. There is then a very rigorous process of testing that is undertaken by the lab to see whether the product actually does provide that. At the end of that process, we review all of that and put out a certification report, which essentially qualifies their assessment as to whether it meets the requirements.

Senator LUNDY—When you say in the lab, is that their lab or your lab?

Mr Scotton—That is the commercial facilities lab.

Senator LUNDY—Is that lab in Australia? I do not know whether any of those companies—

Mr Scotton—All three facilities—

Senator LUNDY—are Australian companies, are they?

Mr Scotton—They all have facilities in Australia. Some of them also have facilities overseas, but they are separate companies. Evaluations conducted within Australia are considered part of the AISEP program. Evaluations conducted by, say, CSC in the United States, if we wanted to recognise them in Australia, would have to go through a process of mutual recognition.

Senator LUNDY—Once that is done, you review the results of their testing?

Mr Scotton—Yes.

Senator LUNDY—Can you give me a little more detail about that, please.

Mr Scotton—There are a number of different elements. For some of those components, we actually take part. We do witnessing of testing and an inspection of the development environment. A lot of it is down to documentation. We review a lot of that as well. We look at their evaluation records to make sure that they have conducted the tests in accordance with the prescribed methodology. That is essentially the process.

Senator LUNDY—Have any of those companies ever had a conflict of interest issue that they have had to discuss with you?

Mr Scotton—Certainly not in the time I have been overseeing the program, which is only nine months.

Ms Connick—Not that I am aware either, no.

Senator LUNDY—Another point, obviously, made by Optus was that it is really difficult to actually become an evaluator. Can you tell me what these companies have had to go through to become accredited as an evaluator of IT security products and services?

Mr Scotton—In the past, this has been done through an open tender process. We have invited companies wishing to perform these services to put in proposals, which have been assessed against each other. They have been selected on the basis of the knowledge and skills of their people and their ability to provide the services. This will change under an open licensing arrangement, where labs will not be assessed against each other competitively. It will simply be a matter of whether they are able to provide the services. But to perform evaluations, they need to have a knowledge of the common criteria and the methodology. This can be gained through training but also through the practice of undertaking evaluations. We provide some level of training in that area.

Senator LUNDY—A point raised, again by Optus, is that this whole evaluation process is extensive and expensive. Is that a valid criticism? Has it contributed to your decision to go to a more open evaluation model?

Mr Scotton—There is no doubt that the evaluation process is long and can be a quite expensive process. It is almost built into the system because of the rigour and the formal processes involved. It can be speeded up enormously depending on the experience of the developer or vendor going through the process. A lot of people going into it do not realise what obligations they are under to provide documentation or testing or other things. At the moment, we are going through a process of looking at the certification process that we undertake within DSD. We think it will have flow-on effects to the evaluation process. It will still be a lengthy process simply because of the rigour that is applied. But that is part of an international standard. I think you will find that, for similar evaluations taking place in other countries that operate similar schemes, the length of time and the cost are comparable.

Ms Connick—Another important point to make is that there are seven different levels of evaluation. Obviously evaluations done at the top level take longer. But there is also the option of having a lower level evaluation, which is not as expensive and does not take as long. As Michael said, we have also found that, in particular, once a company has been through an evaluation, a second evaluation is often a lot faster and easier for them because they develop a product that will pass easily through an evaluation. One of the problems we find often is that we find a defect or a problem with a product and the people that have produced the product need to go back and make a change to make it secure. Obviously, that can take a long time and delay the evaluation process. They go back and modify the product so that it will pass. The second time around, that tends not to happen as much.

Senator LUNDY—What happens, for example, where patches are issued for certain software that are part of a security product? Does it mean they would need to be re-evaluated? How would that work with something like open source if there is continual work or improvement on that software, not necessarily fixing problems but enhancing its functionality over time?

Mr Scotton—We have a subprogram of the AISEP which is called the AISEP certificate extension program. This essentially means that rather than having a product re-evaluated, depending on the scope of the changes, it is possible to go back and assess the security impact of them and issue a certificate extension, which essentially says that the same level of assurance can be maintained about the product. If the changes are outside that scope or if they specifically add new security functionality requirements, that would require re-evaluation. But the important thing to remember is that re-evaluation does not mean starting from scratch. If the product is

substantially the same, there is reuse of existing material and it might be a relatively painless process.

Senator LUNDY—Is that re-evaluation and certificate extension handled by the companies accredited for that purpose, or is that something you do internally?

Mr Scotton—This is currently done by DSD; it is done by the certification group. But as part of the mutual recognition arrangement, there is an assurance maintenance component that is being developed that will have mutual recognition with other countries. At the moment, that is only done in Australia.

Senator LUNDY—It is only done within Australia?

Mr Scotton—Other countries do it, but we do not recognise the certificate extensions performed by other countries.

Senator LUNDY—I want to turn to the protective security manual, ACSI 33 and the discussion we had about Fedlink and alternatives. What distinction is there at all between a VPN and an open network in those regulations?

Ms Connick—I am not sure.

Senator LUNDY—I am happy for you to take that on notice. You have given me some clues about how you would assess that with this whole of facility versus part of the facility. I think that is part of it.

Ms Connick—You can use a VPN over an open network. It is one of the ways of securing an open network.

Senator LUNDY—Do those regulations recognise that as an added layer of security? What Optus say, and certainly my understanding of it, is that there is no distinction between a VPN and an open network other than your evaluation of a particular secure environment or security package.

Ms Connick—There is probably not a lot of detail on VPNs in either ACSI 33 or the protective security manual, but it says that if you want to use open networks to communicate classified information, you need to talk to DSD about the sort of encryption that would be used.

Senator LUNDY—Which comes back to deciding what gets the tick and what doesn't, which is the point they are making?

Ms Connick—That is right.

Senator LUNDY—The question then becomes: given Fedlink has been approved for different levels, including the higher levels, what are you able to do, given you accredit all of these evaluators and providers and so forth, to make sure that that opportunity for other providers is there to secure that type of accreditation?

Ms Connick—The way it would normally work is that a customer agency would come to us and say, 'We want to use a particular VPN solution to transmit classified information over a public network. We want to use this particular VPN, which might include evaluated product and other set-up.' We would talk to them and say, 'Yes, you're using a good product. You are setting up in the right way. We think it is reasonable for you to go and do that.'

Mr JOHN COBB—What are the physical boundaries of your responsibilities? Are there any Commonwealth departments at all that do not come under your eye? When there are contractors working with or for the Commonwealth, are they yours as well?

Mr Merchant—In theory, yes—not that we control all of the activity that goes on.

Mr JOHN COBB—You do not audit what they are doing in this department?

Mr Merchant—We do not audit.

Mr JOHN COBB—You do not check?

Mr Merchant—If we are asked to, though, we can provide an advisory service to them. As Lynwen said, if they are interested in using a particular communication mode and they want to use that to pass either sensitive or classified material, we do not have any boundaries and say, 'No, you department of X, Y and Z are not part of our interests.'

Mr JOHN COBB—Do you check the systems of all the various departments from time to time, or only when you are requested to?

Mr Merchant—We do not check the systems of all departments from time to time. We do maintain control to ensure the integrity of any Commonwealth government system that is going to be carrying very highly classified national security information. Our role below that level is much more of an advisory, education and assistance role rather than an audit and enforcement one.

Mr JOHN COBB—Even in the highly classified areas, you do not automatically check it every so often?

Ms Connick—On a classified level we do.

Mr Merchant—Yes, we do. That is what I am saying; on those we do. Once you get below top secret and secret levels of classification, our role is much more dependent upon other departments taking the initiative to come forward with what their particular requirements are.

Mr JOHN COBB—If a contractor is doing work for a highly classified area, you do not have to approve their security systems?

Mr Merchant—For a company working on something that is secret or top secret, we would have a very close interest in ensuring the integrity of that type of operation.

It gets down to our core responsibilities in information security. We do control that. We do not control the rest of it, though. Tax and Health and whoever have privacy requirements around their information. We are much more of an adviser rather than an audit function of their systems. That is their responsibility, basically. But we can advise them on appropriate products through the evaluation process. We can also, if they wish us to, check on the operation and management of their systems. We do that from time to time, although generally our work in terms of assessing the security of Australian government systems has been more focused on those that deal with material that has a national security classification.

Ms Connick—We have been asked occasionally by the audit office to participate as a technical adviser in audits that they conduct. That is the only time when we really get involved in anything that you could call auditing as such.

CHAIRMAN—Senator Humphries, do you have any questions?

Senator HUMPHRIES—No.

CHAIRMAN—Thank you very much for coming along and talking to us once again. If we have further questions, you won't mind if we put them to you in writing rather than have you come back again?

Mr Merchant—No, absolutely, or we would be happy to come back again if we have not resolved some of these issues. I know there is still a sense of uncertainty about the Optus comments.

Senator LUNDY—I think there were a couple of questions on notice through my questioning.

Mr Merchant—To us?

Senator LUNDY—Yes, I think so.

CHAIRMAN—Look at the transcript to see if there were.

Senator LUNDY—Look at the transcript. But any further clarification about particularly the treatment of VPNs for the purpose of, in your words, creating opportunities for the market to respond, would be helpful. I am just not completely convinced that the evaluation system and the whole accreditation process allows for those opportunities in any meaningful way. To put a finer point on it, I am particularly concerned that the same barriers that exist now will be even stronger as agencies and departments further explore open source software.

CHAIRMAN—Thank you very much.

[12.14 p.m.]

RUSSELL, Mr Calum, Group Manager, Microsoft Pty Ltd

CHAIRMAN—I now welcome the representative from Microsoft who is appearing at today's hearing. Mr Russell, we have received your submission, for which we thank you. Do you have a very brief opening statement? If you do, I just point out that we think our questions are generally more important than statements.

Mr Russell—I have a three-minute opening statement. If that is too long—

CHAIRMAN—We could incorporate it in *Hansard*. Would that be okay?

Mr Russell—If that suits the committee.

CHAIRMAN—There being no objection, we will incorporate your opening statement in *Hansard*

The statement read as follows—

Mr Chairman and Committee Members:

On behalf of Microsoft Australia I would like to thank you for the opportunity to address this important public hearing.

My name is Calum Russell and I am the Solutions Marketing Manager for IT Infrastructure at Microsoft Australia. In this capacity I am responsible for Microsoft's overall position on security and trustworthy computing.

I am qualified to speak about many technical aspects of our software products. I understand that I am before you today to talk primarily about our commitment to what we call trustworthy computing. I would like to mention at the outset that I am not a licensing specialist, nor am I an expert on legal, competition and policy matters. And, while I have a broad understanding of our government business, I do not have a detailed knowledge of its entire scope.

I will certainly do my best to answer all of your questions. If they fall outside my field of knowledge, I would seek the Committee's leave to have my colleagues provide you with the relevant information as soon as possible.

Information security is one of the most complex and pressing issues facing modern, industrialised nations. It involves all aspects of technology. What was once merely a concern for academics and computer experts, now impacts every single person in an information society.

Although Microsoft products are a relatively small - albeit crucial - part of the vast technology business environment, the company has invested considerable resources towards the goal of secure computing. And we are actively engaged with the Australian government on security issues at a number of levels.

As a software company, Microsoft clearly believes in the value of its products. Our US$5 billion annual investment in research and development helps ensure those products are increasingly innovative and secure.

We also believe in the strong downstream economic benefits our software provides to the Australian economy. The Microsoft business model fosters collaboration with our local partners and results in mutual benefits. In fact, we have over 14,000 Australian companies. For these businesses, sales of our software are estimated to drive more than A$4 billion in annual services revenues.

Microsoft's products are used extensively by Australian governments, businesses and consumers, making it a high-profile player in the Commonwealth's technology business environment.

We have significant and valued relationships with many government agencies. We take these relationships very seriously and know that trust and security are the cornerstones for their success.

Microsoft is deeply committed to assisting the Commonwealth in any way we can to preserve the security and integrity of its data.

But it is worth noting that software represents only about 10 % of the entire technology business environment. In contrast, staffing typically comprises 50 to 70 of the total cost of ownership for any IT system. IDC conducted a study of the Australian government IT spend and found that Microsoft software comprises approximately 2% of the total spend.

Infrastructure networks, hardware and services provided by companies like Ipex, EDS, IBM and Telstra are among the major elements that make up the rest. This is why systems security is so complex and requires the close cooperation of multiple players.

Microsoft has done much over the last two years to help design a safer and more secure computing environment. This company-wide effort is known as the `Trustworthy Computing Initiative'.

Launched by our chairman, Bill Gates, in 2002, it followed several years of work to address security at a number of levels. Trustworthy Computing Initiative was based on the recognition that our society's increasing dependence on computers makes us vulnerable to cyber attacks that may threaten the physical and economic well-being of governments, businesses and individuals.

It is clear that the IT infrastructure of the Federal Government has, like the rest of Australia's information economy, become an extremely complex and massive `business environment'. It is comprised of different products, vendors, technologies, policies and procedures.

Microsoft sees this diversity as healthy. In fact we welcome the current debate regarding different products and different approaches to software development.

Our review of earlier testimony shows that this Committee has shown a great deal of interest in the benefits of commercial software versus non-commercial, or `open source', software.

As a commercial software vendor, Microsoft has co-existed with open source products for a long time. We have even looked at ways of adapting the best practices of the open source community to the benefit of our customers.

It is our view that we will continue to co-exist with open source. We will also continue to support neutral government procurement laws. Purchasing decisions should be based on the merits of competing products and on the `fit for purpose' suitability test to which the Australian Government subscribes.

In this context I would like to emphasise one important point. There is absolutely no doubt that security challenges exist for both open source and proprietary software. Software security is an industry-wide problem. Flaws are no more or less prevalent in either commercial or open source software.

Microsoft's high profile means that security vulnerabilities in our products tend to attract media attention that is arguably out of proportion with the reality of the problem.

In fact, a balanced comparison of the number and severity of security vulnerabilities in commercial and open source software shows approximate parity between the two.

One of the claimed advantages of open source software is the fact that anyone can examine the source code, identify security flaws and propose security fixes. However, this so-called `many eyes' approach does not guarantee security.

This was illustrated in the 2002 report of the Computer Emergency Response Team (CERT), a global organisation that tracks security vulnerabilities in computing. CERT said that there were five major security vulnerabilities found for Microsoft Windows, 12 for Red Hat Linux and 12 for Sun Solaris

Some open source software relies on volunteers to create and distribute patches for security vulnerabilities. These are not always rigorously tested before release. Indeed, sometimes they create more vulnerabilities or software incompatibilities than they solve.

Governments now rely on internationally recognised certification programs to evaluate software security. But few open source programs have undergone rigorous security evaluation through programs such as the AISEP process.

The Common Criteria is an internationally endorsed IT security standard that governments - including Australia - use to define their security needs. It helps governments objectively evaluate the security claims of specific IT products before making their software purchasing decisions. Microsoft has attained Common Criteria certification for two of its key operating system products, Windows 2000 Professional and Windows 2000 Server.

Operating system software is a complex creation. It will always have vulnerabilities and be subject to external threats from viruses and malicious attacks. Just as flu vaccinations change every year, software security solutions are constantly evolving to deal with new threats. Consequently, the IT industry is in a perpetual battle. Companies like Microsoft are investing more and more to make their software secure while criminals become more sophisticated in their approaches to hacking.

No vendor's platform is immune. This is evidenced by the fact that computer viruses and worms over the last few years attacked various platforms. They included the 2000 I Love You virus that caused US$8 billion in damage worldwide, the Ramen and Lion worms that attacked Linux software and the Code Red virus that attacked Windows server software.

Microsoft is responding to the threat of cyber-attacks in a number of ways. We work with industry leaders and governments around the world to identify security threats and share best practice. We also assist government agencies at an operational level to prevent and investigate cyber attacks.

In addition we participate in many multilateral forums such as the OECD and ITISAC to share information. As another example, Microsoft Australia was a key participant in the US-Australian Cybercrime bilateral in August 2001.

While security certainly gives rise to real and very serious threats, it is also an area Microsoft views as providing potentially great commercial and economic benefits. In other words, as well as protecting businesses, secure software can help build new business opportunities.

Microsoft's Trustworthy Computing Initiative aims to increase the reliability, security, privacy and integrity of computing. The principles of Trustworthy Computing are at the heart of Microsoft's culture. The company is working to create products that are secure by design, secure by default and secure by deployment. Microsoft calls this 'SD^3'.

Secure by design means prioritising security in the product's initial design. As part of this process we recently stopped Windows development for two months to allow more than 8,500 Microsoft developers to conduct intensive security analysis of millions of lines of Windows source code.

This unprecedented initiative, estimated to have cost up to US$ 100 million, indicates just how seriously Microsoft takes cyber security. We are now conducting similar security reviews for our other products.

Microsoft is undertaking more threat modelling and code reviews, including sharing our source code with third parties under our Shared Source Program. We have taken this program a step further by launching the Government Security Program so that key government security agencies have access to our source code. We are in negotiations, as we speak, with the Defence Signals Directorate about Australia's participation in this program.

Although we have always worked hard to disseminate patches to users immediately, we are continually improving the process. For example, any Windows XP user can be automatically notified when critical updates are available, and they can then easily locate and install a patch.

Microsoft is also focused on a strategy to improve security in the longer term. The Next-Generation Secure Computing Base (NGSCB) is the new security technology for the Microsoft Windows platform.

It is being developed in consultation with the community and uses a unique hardware and software design to give technology users additional security and privacy protection.

With specific focus on system integrity, transparency and interoperability, NGSCB will be integrated into a future version of the Microsoft Windows operating system. It will be a subset of Windows functionality, designed to protect information from interference. You will hear more about this in the future.

Finally, I would like to reiterate that Microsoft is keen to do all that we can to work with this Committee, government agencies and others towards a more secure computing environment, which I'm sure we agree benefits us all.

Thank you.

CHAIRMAN—Thanks for that. You said this in your submission:

Many open source advocates argue that the free software model provides for a higher level of security and integrity than would otherwise be available. Microsoft believes that this is an overly simplistic view, and that the very real security risks associated with the open source development model are often ignored. There are important issues around security that should be examined in this context.

Would you like to talk to us about that.

Mr Russell—Yes. Security is a complex issue. It is very difficult to look at open source versus commercial software in the Microsoft sense on absolute numbers and to say, 'Well, there are so many vulnerabilities and so many vulnerabilities of the other.' We have to look at the deeper level around the operation, the technology itself and the implementation of that of the technology. In an open source context, if we actually take a simple view, for the first stage, of pure number vulnerabilities from one against the other, the matrices coming out show that open source is not without its vulnerabilities. Studies from organisations like CERT—the Aberdeen group have also done the study—show that there are more vulnerabilities coming out in the distributions of open source than there are in Windows in the Microsoft code. This has been prevalent over the last year and a half, so it is not something that is new; it has been there for a while.

They also have to look at the development model of open source and the role of the individuals in this development model. At Microsoft, we invest a lot of our resources and money in building security professionals whose sole objective is to review the code and make sure that that code is secure before we release it. That is maybe not the same in the open source world. The other side to look at is when a vulnerability does occur, what happens? What is the process for responding to that vulnerability? Who is goaled with making sure that that happens, that it is regression tested, that it actually is compatible with the current network and that it will do what it is supposed to do? Once it is deployed, what is the process behind the scenes to make sure that whoever wrote that vulnerability, because a development team made it, are corrected and educated about what mistake they made and build that back into the process to make sure that we constantly review this? It is a moving target. It is not something we can stop and say, 'We've fixed it.'

CHAIRMAN—You talked about the vast amounts of money you spend on examining security. In your submission, you said that you shut down 8,500 Windows developers for a couple of months, costing so far about $176 million. You conducted security reviews of all kinds of products and lines of code. Could you tell us how extensive that was? Was it just a look, or did you change a lot of the 8,500 different products?

Mr Russell—There were 8,500 developers, so individuals, people.

CHAIRMAN—Sorry.

Mr Russell—It was across the one range of products. It was across our Windows server and Windows desktop product. There are 8,500 developers in that community. They took time to review line by line the code. It was not just a look. We had proven that just having a look was not working. We needed to go deeper. One of the first phases in that was education. We thought it was critical to take all these developers back to some of the basics and say, 'How do you write secure code? What are the vulnerabilities and where are they being exploited?' to make sure everyone was on the same level of understanding. It was then a matter of taking them back to their coding job to review the code they have and to work with third parties and the other auditing companies to look at the code to say whether they have also seen anything wrong with it.

CHAIRMAN—How many openings did you find?

Mr Russell—I do not have an exact count, but there were a few openings found.

CHAIRMAN—A few or lots?

Mr Russell—Lots is probably a better way of phrasing it. I do not know the exact number, but I know it was not one or two. There were vulnerabilities found. Our job is to make sure that that goes into the normal process of how we patch vulnerabilities. You would have noticed in the middle of last year, 2002, there was a spate of patches released for the Microsoft platform. A lot of that was the result of that exercise. We also did build it into our new operating systems as we move forward with development.

CHAIRMAN—One thing that I do not understand exactly is with 8,500 different suppliers writing code, how on earth do you ensure that they do not leave the family fold, so to speak, and go out and become professional hackers?

Mr Russell—From the side of working with our developers, we build a very strong development community inside Microsoft and outside Microsoft. It is a strong commitment of ours to take that knowledge that we are teaching our own developers and expose it to other party developers. All the knowledge, the training built for these developers, we actually released in a published book. We believe that the more the developers can get the experience of how to write better code, the better the end result will be for all information technology. Obviously, it is very difficult to prevent one person who decides that they are going to turn into a hacker and a criminal and do damage.

CHAIRMAN—Has that happened?

Mr Russell—To my knowledge, no.

CHAIRMAN—No-one has benefited from being on the inside to go outside and attack?

Mr Russell—Not to my knowledge.

CHAIRMAN—I will ask one more question. Government data stored in proprietary format like Word can only be accessed by someone using the appropriate software. Over time, the company that made the software could go out of business—it happens—or cease to support that particular format. It might be something other than Word, if you think Microsoft is going to be around forever. If that happens, the data becomes inaccessible. That is a very important issue for government in archiving information. What are you doing to ensure that in 50 or 100 years we will be able to retrieve data stored today?

Mr Russell—It is a good point. We are very cognisant of the fact that Microsoft has a long history with different versions of our products. We also know that there are a lot of the older versions installed. It is in our best interests to make sure that we maintain compatibility so that these customers see value in upgrading to a new version and an ability to bring forward their documentation. At the same time, we are investing in open standards in document format. So Microsoft Word has the ability to store in XML formats, which are recognised through the industry as the standard. So other applications and vendors would then have the ability to view that document without the need to use any Microsoft products.

CHAIRMAN—You are confident that 100 years from now we will still be able to access data that is stored using Word?

Mr Russell—Yes, I would be confident we could do that.

Ms PLIBERSEK—According to the Symantec online virus encyclopaedia, they have released over 1,600 security responses for viruses targeting your products compared with 12 for viruses targeting Linux and two for viruses targeting the Unix operating system. Can you tell us what that disparity is about?

Mr Russell—I have not seen the exact numbers from them, so I cannot comment on whether they are right or not. I have seen that that is a common trend. Microsoft operating systems and Microsoft platforms are very popular, as we know. If I were a hacker or a virus writer, the trend would be to write something that does the most damage. The most damage is done by writing it to a Microsoft platform.

Ms PLIBERSEK—You think those figures reflect the uptake of the different operating systems anyway?

Mr Russell—I think definitely that trend is in there. There has definitely been the sheer popularity of the software. I think also that there were a lot of times in the past we were very keen to make software as usable as possible and make it easy to get access. It means when you go back five or 10 years ago, the landscape of when that software was written at that time has changed dramatically to our current landscape, where we are with the Internet being so prevalent and the increase in the number of people trying to damage it and to destroy information. So we have seen that the technology has also moved on. If there are people using an older version of our software that was designed to be more open, it probably also would be easier to exploit that. Therefore, if I were a virus writer, that is what I would write to.

Ms PLIBERSEK—We have had some evidence that you have improved the timeliness of developing patches. Do you want to tell us about that.

Mr Russell—We have taken a hard—

Ms PLIBERSEK—It was a criticism.

Mr Russell—It was a criticism, yes, and I believe there is fair criticism on that. We are not alone on that problem. It is prevalent across the total industry, the timeliness of releasing patches. We have looked at the whole mechanism of releasing patches. We have recently released a document describing what we want to do in the long term. We do not believe we are there right now. That document is in your handouts on patch management. Our process now is to go through a rigorous testing process to make sure that what happens is in our customers' best interests. If a vulnerability gets reported to Microsoft—we get about 10,000 reports a year of perceived vulnerabilities—they go through an evaluation first to see whether they actually are a vulnerability. About 1,000 are found to be something that needs further investigation. The majority, 90 per cent, are user problems or some other documentation error, where we should have said something different in the documentation. So 1,000 go through the next stage of evaluation, which means we have to be able to repeat it. If it is repeatable and comes down to

being a vulnerability in the Microsoft layers of the operating environment, we take it to the process of patching. Once we have taken it through the process of patching, it then goes through the process of being tested fully before being released to our customer base.

Ms PLIBERSEK—What would the turnaround time for that be now?

Mr Russell—It varies on product and complexity of the problem. Some problems are incredibly complex to fix.

Ms PLIBERSEK—What would the range be?

Mr Russell—We have seen some problems take six months while other problems we have seen repaired in 24 hours. There was a recent one repaired in less than something like six hours, where we went from reported vulnerability to patch installed. So it ranges dramatically. It also relates to the importance of it.

CHAIRMAN—You could say it should never have happened, couldn't you?

Mr Russell—I would love to say that the vulnerability should never have happened.

CHAIRMAN—Six hours?

Mr Russell—Yes. It was one that was relatively simple. It also depends on the impact. Some vulnerabilities do not have the same impact. We have a whole system of rating vulnerabilities. We can go out and say if it is a critical vulnerability, it obviously has to be resourced differently from one that we would say is a low vulnerability. It also depends on whether it is in the public domain or not. This has been a large discussion point. If the virus or the vulnerability is in the public domain, it is more important that we repair that quicker. If it is not in the public domain yet, we do have a longer time to repair it.

Senator LUNDY—What is Microsoft's relationship with the Defence Signals Directorate?

Mr Russell—We work extensively with the Defence Signals Directorate. We are submitting our products through the certification process, so the Windows 2000 Server and Professional are currently in process. We have been involved with them on a number of fronts and in a number of different areas.

Senator LUNDY—Like what?

Mr Russell—I am not across every single operation in any of the work with DSD. It would probably be better if I referred it to my colleagues.

Senator LUNDY—Take that on notice.

Mr Russell—I will get you an answer to that.

Senator LUNDY—In terms of your work with DSD, how long does it take to get Microsoft products evaluated?

Mr Russell—It is an extensive process. We obtained the common criteria certification for Windows 2000 just after the middle of last year. That is at the stage where we can then submit it to DSD. It was submitted some time before that. We are still working through the last process in it. Previous submissions have taken over a year without result.

Senator LUNDY—So how does that impact upon your ability to sell the licences for those software products within the public sector?

Mr Russell—It definitely does have an impact.

Senator LUNDY—How?

Mr Russell—I would not be able to quantify it.

Senator LUNDY—But it does not stop you from selling.

Mr Russell—It does not stop us from selling. Our products are used in a number of situations where that level of security is not needed. It does impact our ability on some of the projects. It negates the level of that security. Where we need the security certification levels, it does impact our ability to sell the product there.

Senator LUNDY—As new versions come out, like XP, for example, at what point do you submit that for evaluation? As soon as it is launched? Do you hope that an opportunity for perhaps a job with a high security requirement does not come up too quickly? I am interested in how that whole exercise impacts on you as a vendor for commercial software packages.

Mr Russell—Because of some of the complexities involved and the time and resources involved, we do not submit every single product. It has not been a trend to say, 'Here is every product,' and submit all of our products. We make a selective choice on what we are going to submit. At that stage, it was Windows 2000 Server and Professional. Some of the products will take a while. We are waiting in some cases for them to go through the common criteria of certification first. That is not a quick process either. The two processes back to back mean anywhere from two to three years after the release of the product is when we would expect to see it on the list. It is something we would like to explore if there were opportunities and other ways of expediting the process. It is not easy. We do not want to remove the level of certification but to make it a less onerous, easier process to submit the products. So we have not submitted a lot of products through because of the complexity.

Senator LUNDY—Given all the rhetoric—but indeed there is probably a trend in there somewhere—about going to a more networked environment and that desktops will become units through which you attach to a network as opposed to a standalone model, what is Microsoft's assessment of the security implications of that change, particularly with regard to how you choose which products you get evaluated and how not to? There is a scenario developing that it does not matter what is being used where, it is going to be fully networked; the network is the computer, or whatever the ads say now. How does that impact on how you manage your security evaluations for your products?

Mr Russell—The approach we are looking at is one of what risk there is in the particular use of the products. A desktop product is traditionally behind a firewall, virus checking and a lot of the other processes. It is the same with the applications themselves. There is already a layer on top of that. Our critical point is to look at the systems that are going to be in the line of the security contact with the Internet or the connectivity and then working with other vendors as well to make sure that across the board there is that protection. For something like a desktop operating system, you need to install antivirus software on that to really be secure or to protect yourself from viruses.

There is also the central role the server is playing in authentication. It is a critical part that we are authenticating as a connectivity to the server. That is in our submission. The server piece of software is the whole authentication service. The use of certificates as well is something that is important to us. It is important that we make sure that is supported equally. So I am not sure if that directly answers your question.

Senator LUNDY—I guess it starts to. With Microsoft obviously providing more services in the area of networks and networked computers, when you are sitting behind the firewall, you can make choices about what you do and do not get evaluated and accredited. But when you start to play a stronger role and offer more products in that networked environment, obviously that pushes up that security imperative for you as a company. It is your response to that particular challenge. What are you doing to respond to that specific challenge?

Mr Russell—There are a couple of ways to look at it. There is the certification side of getting through on the EPL common criteria. The other side is the process we are following on building the operating systems and releasing them. To give it a name, trustworthy computing was announced by Bill Gates in 2002. He said it is an initiative that he believes is critical for Microsoft and for the industry—so there are partners in the industry; it is open to other people—to work through. The three core tenets of that are in the design, or the way we build our software, so it is secure by design. That is part of taking our developers through certification. Another is making sure we have the process around what happens if a vulnerability is discovered. A third party audit is an important piece in that. The shared source initiative allows government agencies to view the Microsoft code for our operating systems and work with us.

Senator LUNDY—They are the three elements of the trustworthy initiative?

Mr Russell—Those are the three elements of the design. The next one is the settings of it, the secure by default settings. That is a critical change for Microsoft from saying, 'Here are applications that immediately open themselves up for more connectivity.' The trend now is to say, 'Lock them in their secure mode. Make it easier for a user to set it in a secure environment by making its default secure.' The last setting in that is the deployment one. That is about how we deploy patches and how we actually make sure we keep systems up to date. It is fine if we do all that work up front and deploy it. I would love to say there would never be another vulnerability, but we have to face reality. The software development process is such that we will hit them. It is how we respond to that in the most timely manner and making sure that we deliver the best customer experience. So really secure by design, secure by default and secure by deployment are the three cornerstones where we are talking about part of our trustworthy computing.

Senator LUNDY—On the last point in particular, secure by deployment, you mentioned before there are many different versions of Microsoft's operating systems and applications out there. What methodology do you use to reach your customers, past and present, when you become aware of the need for a patch on security grounds?

Mr Russell—There are a couple of steps we follow when we need to inform customers. We are assuming we have got to the stage where we announced there is a new patch available. I will take it from there. Our first step is to announce that across a subscribed-for-email newsletter service or alert service. That is a free service; anyone can subscribe to it and say, 'I want to hear security alerts.' That is now sitting at 250,000 to 300,000 subscribers worldwide. We have around 10,000 individuals in Australia who subscribe to that service. That is one mechanism and that very quickly sends an email to everybody saying, 'There was a new vulnerability discovered. Here is a link for the patch and here are some instructions and information on what it will actually do.' It all happens concurrently. The second one is working with our product support people. They proactively contact customers whom they have an agreement with to provide these services. They contact them and take them through it and say, 'There is a new patch. Here is the scenario. You should be applying it and this is what you should be doing.' We also announce it, obviously, all over our Internet service as well.

Senator LUNDY—With that product support, I know Microsoft works through many, many vendors and suppliers of your products who, depending on the arrangement, end up doing a lot of that service and installation and all of that kind of thing. Who carries the liability in those circumstances for the nondeployment of a patch? I am presuming you have done this bit. If it is not installed and something goes wrong, is there any comeback for Microsoft?

Mr Russell—Liability is a complex legal area. I do not think I am really in a position to talk through a policy on the liability side. We need to recognise the role of all parties in deploying a patch. There definitely has to be a responsibility on the user of that system to either allow a vendor to automatically update it, which is not what most people prefer to have done, or they have to have the responsibility themselves to take the patch, regression test it in their own environment and deploy it. There are a tremendous amount of policies and procedures and people angle to this problem. I think we have invested a lot of our resources and time on education. We do have through our services and consultants the ability to go through and work with our customers to help them design and build their processes and procedures to make sure that the patches are deployed in a timely fashion and correctly.

Senator LUNDY—Thanks for that. Could you take on notice a bit more information on how that liability structure works. It is a huge issue, I know, so maybe focus on the deployment and installation of patches in particular. Finally, I would like to ask for some more information about Microsoft's shared source initiative and what that actually means.

Mr Russell—We brought through the shared source initiative to give our customers the ability to review our code, to look better at how they deploy it and integrate it with their current environment and as a method to give us feedback and look through it. So there are a number of companies throughout the world that have subscribed to our shared source initiative and get access to the code. The one piece that does not go through gives you all the security components.

Senator LUNDY—It doesn't?

Mr Russell—It doesn't. So there is an extension to that with the government security program. With the government security program, we then open up the security components that we have licensed ourselves, not third party ones.

Senator LUNDY—To government authorities?

Mr Russell—To government authorities.

Senator LUNDY—But not to other shared source partners or whatever?

Mr Russell—We would have to take each one on through evaluation. There are certain companies that would fall into those criteria. This is particularly an extension as a government security program.

Senator LUNDY—Is that your government security program, or is that in response to regulations and requirements in different jurisdictions?

Mr Russell—It is our government security program.

Senator LUNDY—Microsoft's policy is to show government authorities the aspects of your code that relate to security?

Mr Russell—Yes. We open up. It is an agreement that is signed. It is not as simple as just saying, 'Here is the code.'

Senator LUNDY—Is that part of the evaluation process?

Mr Russell—It actually is. That is where we are with DSD right now.

Senator LUNDY—That would only occur when you are seeking to get an evaluation? It would only be for some of your products?

Mr Russell—It would be where we are seeking evaluation. It would also be where we are working on certain projects with the government that might need that access in order to work through that.

Senator LUNDY—You say certain projects. Does that mean you are showing your security source code just to DSD or the relevant authority, or the actual agency or department that you are working with?

Mr Russell—It varies with each government contract signed. Some of them are signed at an individual level. Others are signed as a master or head agreement. Whoever signs the master agreement has the ability to work with other departments as well.

Senator LUNDY—Why is that? Why do you do it like that?

Mr Russell—I am not actually sure why we have chosen that particular way of implementing it. I would have to find out.

Senator LUNDY—If you could respond to that, thanks.

CHAIRMAN—When you were answering Senator Lundy on DSD approval times, it crossed my mind to ask you how Australia compares in terms of product security approval with, say, the United States or England or any other major international player in government circles that extensively uses the Internet and online systems.

Mr Russell—From what I have seen, most governments have some sort of program. Most subscribe to the common criteria and use the common criteria as their base of security. So there is the mutual recognition of common criteria. I am not across each country's individual entry to the EPL, of which each country has their EPL, and the process each one follows in that. I think every single one is different in their process around that. From what I understand, it is not easy in any country. There is not a simple solution to this, but certainly through our contacts, if we come across one that seems to be simpler, less complex but gets the same result, we will happily bring that forward and share it with you to say, 'This is something we have seen work in other countries.'

CHAIRMAN—Microsoft is a very large organisation. Through the organisation, could you see whether there is a view or a range of views out there on how we compare with, say, the United States or England, by way of example, on these issues?

Ms PLIBERSEK—Particularly in relation to time and cost.

CHAIRMAN—That is what it is all about. It is the cost to comply with whatever requirements a government comes up with.

Senator LUNDY—Perhaps we should say to comparable standards.

Mr Russell—Sure. Otherwise it can get—

Senator LUNDY—I thought I had better clarify that.

CHAIRMAN—That is fair. We are not looking for the esoteric. If you could, that would be helpful.

Senator LUNDY—I move that all of the brochures submitted by Microsoft today be accepted as evidence.

CHAIRMAN—There being no objection, it is so ordered.

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.

CHAIRMAN—I thank the respondents to our inquiry and the witnesses. I thank any observers. I thank our secretariat staff. I thank my colleagues and, most of all, as always, Hansard. I declare this public hearing closed.

Committee adjourned at 12.51 p.m.