COMMONWEALTH OF AUSTRALIA

Official Committee Hansard

JOINT COMMITTEE OF PUBLIC ACCOUNTS AND AUDIT

Reference: Management and integrity of electronic information in the Commonwealth

WEDNESDAY, 2 APRIL 2003

SYDNEY

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

Wednesday, 2 April 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 Lundy and Mr Charles, Mr Peter 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

BEZZINA, Mr Mark, Director, Business Standards, Management and Business Communications, IT and eCommerce, Standards Australia International Ltd.....171

CROMPTON, Mr Malcolm, Federal Privacy Commissioner, Office of the Federal Privacy Commissioner.....206

ENGELMAN, Mr Nicholas, Senior Architect, Computer Associates.....143

FERGUSON, Mr Robert Scott, Regional Director, Check Point Software Technologies (Australia) Pty Ltd.....180

HURT, Mr Andrew Bruce Mostyn, Consultant, Check Point Software Technologies (Australia) Pty Ltd.....180

KIDD, Mr David, Solutions Architect, SingTel Optus Pty Ltd.....193

LOVEDAY, Mr Jason, Systems Engineer, Check Point Software Technologies (Australia) Pty Ltd.....180

McCULLOCH, Mr David, General Manager, Government Affairs, SingTel Optus Pty Ltd.....193

NAVARATNAM, Mr Panjan, Projects Manager, Communications, IT and eCommerce, Standards Australia International Ltd.....171

PADDON, Mr Michael William, Spokesperson, Member and Past President, AUUG Inc.....159

PILGRIM, Mr Timothy, Deputy Federal Privacy Commissioner, Office of the Federal Privacy Commissioner.....206

REICH, Ms Jill, Sales Executive, SingTel Optus Pty Ltd.....193

WILSON, Mr Christopher Robert, Regional Manager, Security, Computer Associates.....143

Committee met at 10.05 a.m.

ENGELMAN, Mr Nicholas, Senior Architect, Computer Associates

WILSON, Mr Christopher Robert, Regional Manager, Security, Computer Associates

CHAIRMAN—The Joint Committee of Public Accounts and Audit will now resume 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 everybody here this morning to the committee's third hearing for this inquiry. Today is the last of three consecutive days of public hearings for this inquiry. Further hearings will be held in Canberra in May during the budget session of parliament.

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 houses themselves. 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 a committee statement about the broadcasting of proceedings. In particular, I draw the media's attention to the need to report fairly and accurately the proceedings of the committee. Copies of this committee statement are available from secretariat staff. I now welcome representatives from Computer Associates. Thank you for your submission, which we have published. Do you have a brief opening statement?

Mr Wilson—The terms of reference for the inquiry are wide-ranging, encompassing issues to do with privacy, security, risk management, proof of identity, IT systems, government procedures and processes et cetera. The input from Computer Associates relates to one area where it feels it has particular expertise: the subject of identity management. Identity management brings together threat management and access control systems by effectively and efficiently managing a definitive identity for a user and ensuring they have fast, reliable access to electronic information and applications they are authorised to use. It encompasses authentication, which is proving who a user is; authorisation, which is determining the access rights and privileges a user has; access control, which is managing the means of access; and audit, which is reporting what they have done, real time and forensically.

The benefits of identity management are reduced risks and an improved ability to authenticate a diverse user population; strengthened processes for managing access to and protecting the privacy and integrity of electronic data; dramatically reduced administration costs and improved quality of service; and enhanced capability to respond to changing regulatory and compliance environments, for example, the Privacy Act. We would be pleased to answer any questions about issues raised in CA's submission or indeed on any matters where CA believes it can add some value to the debate. CA is very involved in identity management issues in Canberra, such as the recent Managing Security seminar series that was run there and is continuing to run there and the seminars it is jointly presenting with Ibis Australia on biometric security and identity management to a number of government departments. I would like to thank the committee for the opportunity to present and I look forward to answering your questions.

CHAIRMAN—Thank you. Would you like to tell us a bit about Computer Associates?

Mr Wilson—Computer Associates is a US multinational security software company. We have a number of technologies that revolve around what we consider to be a holistic approach to security management. Those areas are primarily to do with threat management, which traditionally is to do with antivirus programs and intrusion detection, and protection and firewall systems. Most organisations today believe threat management is the primary component of the security of electronic data and systems.

The other areas we specialise in are access control—how you efficiently and effectively manage access to IT resources—electronic data applications and identity management, which we believe to be the overarching approach to enterprise security. Our focus in our submission was around identity management: how do you bring those two together and enforce the policies that should be applied to data.

CHAIRMAN—How many people do you have in Australia?

Mr Wilson—We have about 650 employees in the Australian organisation. We have three development labs—one in Sydney and two in Melbourne. Both of the developmental laboratories in Melbourne are related to our security products, so we actually develop security solutions in Melbourne. The products that are primarily developed there are our identity management and antivirus solutions.

CHAIRMAN—So you have more systems people than you do salespeople?

Mr Wilson—Probably a third of our employees are to do with the development of our technologies in Australia, another third service our customers from an account management point of view and a third are sales orientated people.

CHAIRMAN—As you just said, you focus on identity. You said in your paper:

Crimes covering the theft or misuse of identity and information have been well documented within the Government sector. They range from the recent example of a Centrelink customer with 37 different 'identities', through to ensuring that a passport is issued to the right individual.

I do not think we knew about the 37 different identities, did we?

Ms PLIBERSEK—I think that was in the newspaper.

Mr Wilson—It was in the newspaper, yes.

Mr Engelman—I believe it was Amanda Vanstone who reported it to the *Australian*. It is a common problem with identity management; identity theft worldwide has become a serious issue. At the moment I guess part of the issue is that it is reasonably easy to look up a birth certificate, satisfy your points check and go down and take on the identity of somebody else. There are practices that governments worldwide are starting to look at and address: how can we more securely issue identity and control identity?

CHAIRMAN—For sure, it is a complex task and we do not always get it right. There are a lot of people wandering around the world that we would like to know where they are or who they are. It is not that hard, is it?

Mr Wilson—The issue of authentication is quite a difficult one. The challenge of identifying that you are who you say you are is probably one of the major issues associated with authentication. Typically today, authentication is going quite quickly down the biometric path. Am I who I say I am? The fact that I might have a licence or a passport or some kind of identification paper does not necessarily mean I am who I say I am.

CHAIRMAN—My understanding is that biometrics is not that reliable yet.

Mr Engelman—I would agree with that comment. I think you are facing two problems. The first is that biometric systems have proved reasonably easy to fool. We have got documented cases. For instance, a professor in Japan bought some gum and was faking fingerprints. He was able to take a fingerprint off, for instance, a coffee cup, put it onto a gum and go into a biometric system that was supposedly not going to allow him to go through.

Ms PLIBERSEK—Was he just doing that to prove that the system was flawed?

Mr Engelman—Essentially a proof of concept. I believe he got through something like seven to 15 different biometric systems, all fingerprint based, using about $10 worth of gum that he had purchased.

Ms PLIBERSEK—Do you mean chewing gum or some other sort of gum?

Mr Engelman—It is the stuff that they make Gummy Bears out of—gelatine, I guess. We have had the Safe Gate initiative at the airports quite recently where two Japanese tourists were documented as changing passports and fooling the system.

Senator LUNDY—Is this the Customs biometric program?

Mr Engelman—Yes, that is right. And facial recognition has been shown worldwide to be flawed, certainly at the airports where they have tried to use it to pick up terrorists. The big issue is false positives: they identify too many people who are in fact not terrorists as being terrorists, compared to actually picking up the people they are after. It seems that reasonably small changes to your facial appearance can trick the facial recognition stuff.

Ms PLIBERSEK—Like putting on or losing weight.

Mr Engelman—Absolutely, yes—or growing a beard.

Ms PLIBERSEK—Even growing a beard? That is really an obvious one, isn't it?

Mr Engelman—Nevertheless, at the level they are running to cut out the false positives, it is probably enough to get through those types of systems. Then you can go to the more esoteric systems like in *Blade Runner* where he actually pulled out somebody's eyeball so that he could go through the system. If you look at proving identity there are three things you can have:

something that you know—a user ID and a password; something you have, like a token, a smart card—your ATM cards are good examples; and something you are, which is biometrics.

Senator LUNDY—*Minority Report* was a more recent incarnation of the eyeball trick.

Mr Engelman—I have not seen it.

Senator LUNDY—You must see it.

Mr Engelman—I think there is actually a fourth one as well, and that is where you are. If I am suddenly getting credit card transactions being made in the States whilst I can prove I am in Australia, obviously they are fraudulent. But they are all issues that identity management, and particularly authorisation, need to look at. So it is authentication and authorisation. Once you move into the electronic realm they become really difficult because you need to control the mechanism where they are being authenticated as well.

CHAIRMAN—The problem, is it not, is that we rejected the Australia card, though I am not sure that would have solved all the problems anyway. You agree with me that biometrics is not yet reliable enough to be foolproof, yet you say that what is required by government is a single solution—and then you have five dot points. So what is a single solution? If it is not putting too fine a point on it!

Mr Engelman—That is a reasonable point. We believe that the single solution has to start at a policy level. We have noticed in some of the other submissions you have received that government probably needs to set an overarching policy in terms of what level of proof is going to be reasonably required to authenticate somebody as they come to transact with government. Once you have that policy in place you are going to have to go through some form of risk assessment to identify the level of authentication required to access various resources. It might be quite trivial for some things; it might be involved for others. Trivial could simply be user-ID password; involved might require the physical presence of somebody.

Once you have identified the assets you are protecting and at what level they need protection, then you would start to look at tools to implement those protections. Computer Associates certainly has a range of tools to help you enforce and implement that policy. However, Computer Associates does not deal with the primary mechanism for authenticating somebody in the sense that we do not provide biometrics; we provide systems that will work off biometrics.

Mr Wilson—Biometrics can be as accurate as you want it to be. Ultimately you could prove that I am who I am by perhaps doing a DNA test or taking a blood sample.

Ms PLIBERSEK—Like *Gattaca*.

Mr Wilson—Yes, like that.

Ms PLIBERSEK—Like Ethan Hawke and Uma Thurman, you could provide a little DNA sample every time you go to work, a little scraping of skin—

Mr Wilson—So that you could do a DNA test and that would prove biometrically that you are who you say you are. But it is impractical. It is the same with the facial scanning system. Depending on how many reference points you want to check—it could be 16 or 64—that is a level of security.

Senator LUNDY—And that is adjustable.

Mr Wilson—That is adjustable. With iris scanning it might be 256 reference points. So it is a balance between what is practical and what is the most effective way of doing a biometric—

CHAIRMAN—You are not telling me that we will never get there, are you?

Mr Wilson—No, I am not telling you that we will never get there.

CHAIRMAN—Science does some miraculous things, doesn't it?

Mr Wilson—Absolutely.

CHAIRMAN—How many years ago was it that we discovered DNA? It wasn't many—10 or 12 years ago, that is about it. I have a company in my electorate that is a very major player in DNA testing, and they started on animals. They had to move to humans because people kept begging them.

Mr Wilson—In general, with security you can have a system that is 100 per cent secure but it is probably 100 per cent impractical.

CHAIRMAN—You have talked about an overarching single government approach to these issues. Have you read the document, *Australian Government use of information and communication technology*?

Mr Wilson—No, I have not.

CHAIRMAN—It is the second report of the Management Advisory Committee of the Australian Public Service. Could you have a look at it, and come back and tell us whether you think that will help set up the kind of solutions that you are looking for?

Mr Wilson—Sure.

CHAIRMAN—You work with PKI?

Mr Wilson—Yes.

CHAIRMAN—Have you had any involvement at all with Gatekeeper?

Mr Engelman—We have certainly been around the edges of Gatekeeper. We have our own PKI solution. We have not chosen to go down the Gatekeeper accreditation route, but we are well aware of what Gatekeeper is.

CHAIRMAN—Do you have an alternative to Gatekeeper?

Mr Engelman—No, we do not. We decided that there were already sufficient players who were Gatekeeper accredited. We would work with those rather than becoming another vendor in that space.

Mr Wilson—Our technology is used in SecureNet's Gatekeeper solution. Our directory is underlying their PKI infrastructure.

CHAIRMAN—Some people and some submissions have argued to the committee that Gatekeeper is far too complex and too expensive for them to implement. Do you have any knowledge or comment about that?

Mr Wilson—It is relatively complex and it is an expensive solution, but one that is necessary if you want to get to the level of security and privacy that is probably going to be required down the track. Today we have a Privacy Act, but is it enforced? I would say that it is not. CA is doing work with HIPAA, the Health Insurance Portability and Accountability Act, in the US. Similar privacy conditions apply in Australia, but they are probably more rigorously enforced in the US at the moment.

Ms PLIBERSEK—Can you tell us a little about what you are doing with HIPAA?

Mr Wilson—Primarily we are working on a solution with a number of companies in the US, and an example is in hospitals. If I was to go into hospital, I would have to have a file created that represented my physical condition, my ailments and the treatments I have received. In the US—I am not too sure about in Australia—they have lots of nurses stations with computers. Theoretically, what should happen is that anyone who accesses the computer has to logon and each time someone's file is pulled down that is logged—say, when a doctor wants to look at my file. It will keep track forensically of who has looked at my file. For example, Chris Wilson can ask, 'Who has looked at my health file?' and the hospital will be able to tell me that. From a practicality point of view, what actually happens is that a nurse logs on in the morning and it stays logged on all day, and the doctors walk up and pull down the files. If you went to look at the end of the day at who accessed what file, it would probably be the one nurse that logged on at the beginning of the day.

While the technology exists to enable people to logon discretely and to track what they do in a system, it is not being practically implemented today. So what CA is working on with a couple of other companies in the US is having a workstation where the doctor or the nurse, rather than having to log on—which they think is onerous and time consuming—would come up and biometrically log on. The workstation would know exactly who that doctor was; it would log the doctor on to the applications and then would track or audit what he does behind the scenes, what files he pulls down. You probably have an identity card or a proximity card?

CHAIRMAN—No.

Mr Wilson—When the doctor moves away, it automatically logs him off, so the next person who wants to do something there has to be biometrically logged on—with a finger scan or other biometrics. That allows them to implement their privacy policy, for example.

CHAIRMAN—What was that movie that was based on the true story about the bloke who, amongst other things, pretended he was an airline pilot and a doctor?

Senator LUNDY—*Catch Me if You Can.*

CHAIRMAN—That is it.

Mr Engelman—The other area where we are involved with the PKI is the Identrus initiative. It is being run by the global banks. It is essentially setting up for the very large business-to-business transactions and providing authentication, authorisation and nonrepudiation—that is, the ability to say that you actually did have this transaction with me. That is a very heavily PKI-centric solution built upon our directory which is using real-time certificate revocation.

Ms PLIBERSEK—What is that?

Mr Engelman—If you think back to the days when you had a Bankcard, you would go down to Myers and make your transaction and they would actually pull out a book and go through it to see if your card had been stolen. That was a latency issue. You probably had a window of a week where you could use a stolen credit card before the next book came out. The same thing happens with public key certificates. Essentially, if someone steals your certificate or it is compromised in some way, you have to publish a revocation list that says, 'This is no longer valid.' One of the big issues for the banks is that they wanted that in real time. A standard was put out called the OCSP responder standard. CA has developed technology to deliver that so that in real time they can say, 'This certificate is still valid.' The transaction is backed all the way back to the initial issuer of the certificate.

CHAIRMAN—Does that take a huge mainframe?

Mr Engelman—No. It depends on the size of your customer base. At least for Identrus that is running on—

CHAIRMAN—It must also depend on how quick the cycle time is too, if you are running a 24-hour clock.

Mr Engelman—With the directory we are building on, the cycle time is pretty much instantaneous: as soon as they enter the information that it is revoked that is published.

Mr Wilson—For example, just on numbers, the Bank of America uses our identity directory technology. They have 25 million customers who are in a real-time banking environment. That is all done with UNIX systems and Sun hardware, for example. In Europe, our identity directory is used by Cable and Wireless for their digital TV subscribers. They manage 200 million subscribers over there. The technology is there and it is an expensive exercise.

Ms PLIBERSEK—What sort of identification do cable TV subscribers need? What do you provide for those companies?

Mr Engelman—I will take a step back. Identity management can mean different things to different people. If I was to talk to one of our customer's technical people, he might think about

identity management as managing logons. I am a user in my company and when I go to access the system, I log on and there is a whole lot of work associated with that logon. In identity management, I would be given a role as a programmer, a manager, a parliamentarian or whatever, and in that role I would have access to all their systems. I am granted access based on my identity. If I was to talk to a CIO—a chief information officer—of a company, he might be more interested in identity management as it relates to provisioning users. If I join a company as a payroll clerk, in that role I get access to all these systems, I get an identity pass to the building and I get a car parking spot. That is how that identity is managed. If I am a digital TV subscriber to Cable and Wireless, I am a customer. As a customer, when I ring up and I have to verify my identity it will not be through biometric identification; it will probably be by saying, 'I am Chris Wilson and I am your customer.' Then they will want to provision me with maybe the next pay TV fight or the Disney Channel for my children or whatever. Managing an identity could be either from a low-level technical perspective or as a customer and then provisioning me based on my identity.

Ms PLIBERSEK—So when you are talking about what you do for a pay TV company, you are talking about software that enables the operators to recognise the account that the person has, what they have already and make additions or subtractions to that?

Mr Wilson—Yes.

Mr Engelman—They will have an addressable smart card in the box. Every customer has a set-top box and there is a smart card that slots into that. Even if somebody rings up and says, 'I am Chris Wilson and I would like this feature,' it will go to Chris Wilson's box and not to the person who might be masquerading as Chris Wilson. If he suddenly sees a service turn up that he has not ordered, he will ring them up and say, 'I did not order this,' and they can reverse that transaction.

Mr Wilson—Ultimately, it could go down to the biometric level; obviously it is too expensive now. I think one of those little cameras is about $350 to look at your iris. Down the track it might be $30, and every time you ring up and you want a pay TV fight, you might have to scan your iris in or swipe your card.

Ms PLIBERSEK—You talk about single sign-on technology—and I can very easily see the attraction of that—but I am concerned that it might be much easier to crack through than something with multiple layers of defence. Can you tell us about that?

Mr Wilson—I will make my high-level comments, and Nick might want to back them up. You are absolutely correct—single sign-on is a fantastic productivity tool; it makes our lives easier. I do not know how many access points you have to different web sites or different systems within parliament et cetera, but I imagine you might have more than one logon ID—you might have 10.

Ms PLIBERSEK—We only have two.

Senator LUNDY—We have two, but it has got better. You also have other optional extras you can put in.

Mr Wilson—At work, you might decide that you want to join the *Sydney Morning Herald* news service, so you would get another one for that.

Senator LUNDY—Yes, so we might have 30.

Mr Engelman—Potentially, with single sign-on, you could have one. Using someone else's term, it could open the keys to the kingdom. Where it does become important is to have hardened authentication out the front of it. That could be biometric; it could be what they call two-factor authentication.

Ms PLIBERSEK—What does that mean? You are speaking to someone who does not understand all this terminology.

Mr Wilson—It means two levels of authentication. One level may be my user ID and the other one might be my smart card, my iris or whatever. You could have three levels of authentication.

Ms PLIBERSEK—You do not just mean a logon and a password?

Mr Wilson—No.

Ms PLIBERSEK—You mean two separate systems?

Mr Wilson—Yes.

Mr Engelman—It goes back to what I talked about a little earlier. There are three mechanisms to authenticate: something you know, which would be user-ID password; something you have—token, smart card, ATM card; and something you are—biometrics.

Ms PLIBERSEK—I have seen little keys that have a constantly changing number that you have to log on with.

Senator LUNDY—They come in two formats.

Ms PLIBERSEK—Can you tell us about those?

Mr Wilson—It is known as a challenge-response system. We work with those. CA tends to sit more at the back end of this. We use these as mechanisms to authenticate into our systems which secure the areas that you are trying to secure—the data and the systems. With a challenge-response token, you go to log on to a site and the site issues a challenge, which is typically a number. You type that number into a little pad, plus your PIN, which proves that you actually own the card and it is not one you have just picked up randomly.

Senator LUNDY—We used to have a challenge response plus PIN. This one now has a changing number, so it is simplified. It is PIN plus the number, which is a time-coordinated number.

CHAIRMAN—Is that for senators?

Senator LUNDY—Yes. There is a time-coordinated number for us in Parliament House. You have to put that number in. It is a bit simpler now than the challenge response was.

CHAIRMAN—If I try and use my laptop outside of the cable environment, it goes to the challenge response.

Senator LUNDY—This is new; this is a pilot that is happening with our remote access. You, too, will have this soon.

Ms PLIBERSEK—Martyn Evans is on the pilot too. That is why we have seen it.

CHAIRMAN—Okay.

Mr Wilson—That is an interesting point because that goes back to another level, a fourth level, which could be where you are. So managing my identity and access could be those three things that Nick has talked about, and the fourth one could be where I am. For example, I am always in Sydney and if, all of a sudden, someone in Melbourne is trying to get into a system or trying to do something based out of Melbourne, the overarching security system would say, 'That does not work: against our policy.' It would be similar to yours when you are out of the office.

CHAIRMAN—I do not care where we are, just whether or not we are on that cable.

Ms PLIBERSEK—It is an extra level. If you are not on your computer at Parliament House, it is an extra level—you get the challenge response level.

CHAIRMAN—Not in the electorate office.

Ms PLIBERSEK—No, not in the electorate office, but if you are somewhere else.

CHAIRMAN—That is why there is a cable.

Mr Wilson—The challenge there is that hackers generally do not get into a system from your office or parliament; they probably come in from another country.

Ms PLIBERSEK—On public key certificates: does that make it harder for, say, Australian government departments to do business with overseas companies or departments? The CSIRO were saying yesterday that their lives were made a little more difficult because they transmit vast amounts of data with their partners overseas and not all of their partner organisations used or understood public key infrastructure and recognised the certificates.

Mr Engelman—PKI is a fairly robust and proven technology but it is not yet a globally rolled out technology. A lot of the world is still in user-ID password mode. PKI has been coming for a lot of years and it is still coming. I think it is becoming a lot more accepted world wide—for instance, it just keyships now in most of the major browsers by default, so if you hop onto the web and try to download some software from somebody you will see that it has been signed by, say, the Microsoft Corporation. That is done by a key already embedded into the browser. So the technology is already starting to become a little more pervasive without us

being aware of it, but organisations looking for a dedicated PKI solution are definitely going to run into applications that are not PKI aware and organisations that are not using any form of PKI. So I think the comment is fair. If you had asked them five years ago they would probably have been much more vocal about the problem; if you ask in five more years it is probably going to be less of a problem.

Ms PLIBERSEK—Is it still worth doing, despite the inconvenience?

Mr Engelman—There are a lot of arguments for and against PKI. My personal opinion is that it is worth doing.

Ms PLIBERSEK—Why?

Mr Engelman—Because I believe it adds levels of security to our transactions.

Ms PLIBERSEK—Can't you get them in another way?

Mr Engelman—It is one of the more efficient ways of doing it. The great thing about public key cryptography is that I do not have to have a secure mechanism for exchanging keys. If somebody like Lockwood issues you a new lock for your house, they make the lock and they make the key together and they give both to you. With the public key infrastructure, I can actually have the lock over here and the key over there and they are interchangeable. It makes it very easy for me to publish the public piece of my key, and anybody who has PKI-aware software can then communicate with me without having to understand anything else about it. That is a poor explanation—it might be better if I send you a document that outlines how PKI works.

Ms PLIBERSEK—That would be good, thank you. We would appreciate it if you sent that to the secretariat.

Mr Wilson—A key issue with PKI is the concept of nonrepudiation. With PKI, I can electronically confirm who I am and someone at the other end will believe me; whereas today, without PKI technology, someone could get on a computer and send me an email and if they say they are Chris Wilson there is no way that they can prove it. With PKI, if I use the right keys and I send an email and attach my PKI keys to it, that will guarantee that I am who I say I am.

Ms PLIBERSEK—Can people steal PKI? How common is that and how would you do it?

Mr Engelman—It is definitely possible to steal somebody's certificate. Certificates are protected by some form of password access to them in a similar way that a token is protected, so it is certainly possible to steal them. However, the most typical way of acquiring somebody's key is actually identity theft and then simply applying for a key. We had a case about a year ago where an organisation applied for a key claiming they were Microsoft and they were actually issued with the key, so they were then able to issue software that was signed as if it had come from Microsoft. That is when we get those revocation lists.

Ms PLIBERSEK—What was the purpose of doing that?

Mr Engelman—It meant they could masquerade as Microsoft. I have no idea what the motivating desire behind it was but they could certainly damage the company's reputation by doing something along those lines. In certain circumstances I can imagine that it would give you a fair amount of power. If I were able to steal the identity of somebody in the financial industry in that way and then start masquerading as them, theoretically I could make some life changing financial transactions.

I would like to address two other things that you brought up. Going back to the question of whether we would require a mainframe to run these sorts of things, the internal government would run quite nicely on a UNIX platform and you could probably get all of Australia into the infrastructure at that level as well. Certainly the technology already exists to provide identity management solutions for a country the size of Australia. The population is not too big to be managing in an identity management space. Those technologies are becoming more and more mature; they are scaling down onto smaller platforms.

Senator LUNDY—A UNIX platform is not a mainframe. It is a different system.

Mr Engelman—That is right. With single sign-on we talked about the keys to the kingdom problem. The argument runs that if you put strong authentication at the front end, which is what Chris talked about, you protect against the keys to the kingdom but you are also removing a security risk. When you have multiple systems that you have to sign into with different IDs and passwords you start getting post-it notes being stored on monitors or under keyboards and so on. There is a strong argument that single sign-in actually reduces security risk. The other way it reduces it is by requiring stronger passwords. When I have to remember 20 passwords I tend to choose easy things to remember.

Ms PLIBERSEK—Or the same password for every system. Someone might do that—I do not.

Mr Engelman—If I have a single sign-on solution I can have one strong mechanism at the front end and I need not know the passwords for all the back-end systems. Good single sign-on systems will manage that for me and assign hard to guess passwords on a policy based basis, so perhaps every 30 days it will change without the user even being aware that it has been changed. It can enhance security greatly.

Senator LUNDY—Does that software potentially sit over the top of everything else? It is password management software, effectively?

Mr Engelman—It is authorisation management. I would go a little bit further: it will present you with only what you are allowed to have access to and it will authorise you to use it.

Senator LUNDY—When Microsoft applications say, 'If you want us to remember this password, tick this box,' is that a form of that type of password management? What does that mean?

Mr Engelman—It is certainly heading towards a single sign-on type of approach but I would argue not a particularly secure one.

Senator LUNDY—I never tick the box because I do not know what it means. I do not know whether that means Microsoft knows all my passwords.

Mr Engelman—It means that it has to store it locally on your system. It will store it, typically, using a one-way encryption so that it is not easy to get it back. But over the years we have seen those being broken. It is not a single sign-on system in the sense of a robust and secure one, but it is addressing the same problem: how to make sign-on easier for users. The other reason you put single sign-on is for efficiency gains. And that is what you are seeing with Microsoft. It is easier to go to sites—you do not have to remember those passwords and type them in.

Senator LUNDY—That leads nicely to my next question. You cite some figures in your submission about the cost of resetting passwords. I am not sure which contract you are referring to but I am aware that under the various outsourcing contracts there is a dollar fee attached to basic work processes, including the resetting of passwords. You cited from $48 to $200 per time. The average user requires approximately 1.5 password resets per year. You then go on to say that there is a 12 per cent turnover rate with government employees. That adds up to a lot of money, doesn't it? That is part of your argument.

Mr Wilson—It is a lot of money. As a software company, Computer Associates, we do a lot of business helping companies and primarily it is around service desks—there are lots of statistics on this—and, by far, Monday is the day when most of the requests for new passwords come in. Someone changed it on Friday, they have had a great weekend and they come in on Monday and think, 'Oh, what was it?' They get on the phone and get into a queue until they get someone and get it reset. There are a couple of things wrong with that. One is that there are a lot of costs associated with keeping that service desk active.

Senator LUNDY—It could lead to a significant proportion of downtime as well.

Mr Wilson—Yes, that person is absolutely—

Ms PLIBERSEK—Especially if it is the CSC help desk.

Mr Wilson—That person is not doing their job because they cannot log in. That can vary from one hour to a day.

Ms PLIBERSEK—Yes: 'We'll phone you back'—sometime next February.

Mr Wilson—It is also a security risk because often they say: 'What is your name? Chris Wilson? Okay, it is reset.' Because they are in a hurry and there is too much work to do they will just reset it. They will say: 'Chris, your new password is Wilson. You are back, active.' Where we are seeing that whole space move to is the idea of self-administration. You probably do it already in situations where you might have to ring up and give your mother's maiden name or birthday—

Ms PLIBERSEK—Or the name of your first pet.

Mr Wilson—You are the only one, supposedly, who knows that information. If you could do that in a self-administration system through the web—for example, you could reset your own password. That is probably a lot more accurate than ringing someone up at a service desk who is rushed off their feet and has 100 passwords to reset on Monday.

Senator LUNDY—Is that current practice more to do with an excruciating business model on behalf of the vendors themselves or is it more to do with the technology itself and the need for someone to have—

Ms PLIBERSEK—Ten passwords.

Senator LUNDY—I guess I am thinking of the systems administrators.

Mr Wilson—It is more to do with the technology today. As a vendor, a software company, we are doing a lot of business around this space because the technology is there today to save money, to make things easier for everyone, et cetera. Part of it was the Internet. Before the Internet came along, if you forgot your password you could not get on to the system to reset it or do anything. Now you can go to someone else's machine and, through the Internet, answer the questions and have yourself reset. Technology and the Internet play an important part there.

Senator LUNDY—In the context of employees and single sign-on, and thinking more from a citizen's perspective, how close are we to citizens having one sign-on into government sites? Or does that come down to the same issues?

Mr Wilson—I think it is a pretty broad issue.

Senator LUNDY—Let me add another layer: single sign-on to the three tiers of government.

Mr Engelman—There are moves to achieve this. At the state level a couple of the state governments are already starting to bring together all of the government information into a single site. You can hit one site, look up which department you want to deal with and fire a sign-on at the opening screen. You can then go and apply for a dog licence or a car licence or a passport or whatever it is that you want to get processed, and so on. It will also allow you to search for information on whom you should be contacting and so on. The move to federate all that information is already taking place. It is something that is being recognised worldwide. That is why our response was focused around identity management because identity management is based on holding certain information only once—the basic static information about me: my name, where I live, my phone number and other contact details. These things that probably do not change too often I would want to hold only once and have all my applications read that from that single source. Once you start doing that you have quite a powerful model to then drive all your services from that. You can base your authentication and your authorisation around that single base as well. It can hold information not only about who I am but also about what I am allowed to do. We are starting to see that happen in government and industry worldwide. It has probably been the hot topic for the last couple of years. It has been around for a lot longer but industry and governments are starting to pick up on it and drive forward on those sorts of initiatives now.

Senator LUNDY—Which are the leading sectors?

Mr Engelman—I think the financial sector probably has a good lead, at least in the business-to-business side. There is also the question of internal versus external. A lot of companies are doing it internally for a start.

Senator LUNDY—From the citizen's perspective, which countries have e-government to the point where they have a single sign-on?

Mr Engelman—We would probably want to come back to you on that one.

Senator LUNDY—I would be interested to know.

Mr Wilson—We will come back to you with a more definitive response, especially on the work that CA is doing. A lot of the Asian countries are a lot further down the track than Australia is on the concept of an identity for a citizen. For example, Malaysia is one. In the past, Malaysia has had a fairly poor reputation for the amount of fraud et cetera going on there. One of the things that they are implementing is the identity card concept so that their citizens will have an identity card.

Ms PLIBERSEK—That is fine if you are a police state.

CHAIRMAN—Hitler was very good at that.

Senator LUNDY—This is the balance: between that ubiquitous identifier—there are issues within Australia and in other places about that—and the practical, functional technology that is effectively a ubiquitous identifier for all citizens but does not carry with it the more obnoxious characteristics. I like to think technology can provide that, but it would have to be in a very carefully designed model. I am trying to get an idea of what models are out there.

Ms PLIBERSEK—If you make it impossible for citizens to access government services without such an identity, the people that miss out are homeless people and mentally ill people. The most disadvantaged people are the ones who already find it difficult to provide paper identity in documents. I guess that is the policy issue as well. You sometimes lock out the most needy people in those circumstances.

Mr Wilson—That sort of issue is a government style issue. The technology is there today to do it and it has been there for a while.

Ms PLIBERSEK—You could microchip people—the technology exists—but would you?

Senator LUNDY—They do that to dogs.

Ms PLIBERSEK—I know. That is why I am saying it exists but you would not want to do it.

Senator LUNDY—Can you have a system that has both—that is, a system that has some sort of technologically driven identifying system, whether it is biometrics or some sort of single sign-on process, and traditional identifiers like your name and address? Can they coexist?

Mr Engelman—Absolutely. I think the strongest form of identity is walking up to a service window and presenting yourself with some form of physical ID that you are carrying and that you have gone through a points check to acquire. Electronic identity always has the question: 'Is the reader secure?' With a biometric solution, I still have the issue about whether it has been compromised at the other end because all it is is an electronic signal saying that it is me.

CHAIRMAN—You said before that we would take our smart card to get into parliament or whatever. In fact, we do not. The security system requires security personnel to recognise each one of us.

Mr Wilson—So that is an added level of security authentication?

CHAIRMAN—It is the only level of authentication.

Mr Wilson—You do not necessarily need your card?

CHAIRMAN—We do not have a card. As there are no further questions, I thank you for appearing today; it has been informative. Again, we appreciate your submission. We will send you a copy of our report.

[11.03 a.m.]

PADDON, Mr Michael William, Spokesperson, Member and Past President, AUUG Inc

CHAIRMAN—Welcome. Thank you for coming today and for your submission. Do you have a brief opening statement or should we start with questions?

Mr Paddon—Please go straight ahead with questions.

CHAIRMAN—Could you tell us about AUUG?

Mr Paddon—AUUG is Australia's peak professional body representing open systems and open source. It has been in existence since 1975. As a consequence it has built up what we regard as a critical mass of experience and knowledge in the arenas of data management, enterprise systems, networking and so on. We currently have some 600 members. That is a brief overview of who you are.

CHAIRMAN—How large is the secretariat?

Mr Paddon—The secretariat consists of one person.

CHAIRMAN—Are you it?

Mr Paddon—No; the secretariat is another person. I am a member. I am sorry, do you mean the board?

CHAIRMAN—Is it just a group of members with no bureaucracy?

Mr Paddon—I am sorry; of course it has a bureaucracy.

CHAIRMAN—That is what I was asking.

Mr Paddon—My apologies.

CHAIRMAN—It was my terminology.

Mr Paddon—AUUG is an incorporated membership organisation. It has a board that runs it that consists of approximately 10 people. It has a full-time staff member, which we call our secretariat, which is why I got confused. It has a number of subcommittees which are created from time to time out of the broader membership to address various issues.

CHAIRMAN—But it has only one staff member?

Mr Paddon—Only one full-time staff member, yes.

CHAIRMAN—You said in your submission:

Public key technology is widely available and AUUG highly recommends the use of this style of authentication technology for access to any valuable or sensitive online information asset or service.

Do you want to tell us a bit more about that?

Mr Paddon—Yes. One of the areas that we thought was very important to talk about in the submission was authentication, because that is the keystone of other sorts of data protection that occur online. There are many forms of authentication that have been used in the past—passwords are very popular. We have seen other sorts of authentication, such as biometrics, hardware tokens and so on, used from time to time in the industry. We feel that public key authentication actually is both significantly stronger in a very real sense cryptographically and in a very practical sense in terms of its utility for providing access to online resources. For instance, passwords, as we all know, can be forgotten or guessed or put on little yellow bits of paper stuck on a terminal. Biometrics are notorious for their false positive rates. Public key authentication systems have none of these problems. They are well understood. They have been in existence for at least 28 years. We feel as a group that they are the best overall answer to online authentication we can recommend to the committee.

CHAIRMAN—Specifically Gatekeeper?

Mr Paddon—We did not mention Gatekeeper. That goes one step further. The Gatekeeper system is about public key infrastructure which involves certificates and so on. You do not need to use a PKI to use public key mechanisms. However, if you want to distribute on a wide basis—say, to the citizens as a whole—you may indeed want to use PKI and therefore you would probably want to use the Gatekeeper standards because they are very good.

Senator LUNDY—Can you explain PGP to the committee?

Mr Paddon—PGP is a software system that was written by a person called Phil Zimmermann some years ago. It relies on public key authentication to sign and encrypt emails or any other form of electronic document. However, it does not require a public key infrastructure to operate. It operates on what is called a 'web of trust', which effectively involves the people in the system assigning levels of trust to people they know and then the people they know assigning levels of trust to people they know. As a consequence, you can establish a worldwide web of trust without having to have a hierarchical tree, which is the idea of a public key infrastructure.

Senator LUNDY—PGP stands for 'pretty good privacy' and it was an open source, public key piece of software.

Mr Paddon—Yes.

CHAIRMAN—One of the things we heard a lot yesterday was how expensive Gatekeeper is.

Mr Paddon—I am not really in a position to comment on that specifically, not having ever attempted to achieve Gatekeeper accreditation myself. However, one of the things I would note about Gatekeeper is that while we feel that the policies and procedures around Gatekeeper are very good, one area where they are weak is that they do not take any steps to ensure an ongoing

alignment between a commercial Gatekeeper provider and the needs and goals of the government and/or the citizens. Obviously, a commercial organisation has different goals from government and from the citizenry as a whole, and it was not clear to us when we reviewed Gatekeeper how that alignment was to be maintained over a significant period of time.

CHAIRMAN—Isn't it possible to steal a key?

Mr Paddon—It is absolutely possible to steal a key, in which case you would simply revoke that key and another one would be issued. That is much better than, say, the biometric approach.

CHAIRMAN—After the world blows up or before!

Mr Paddon—Private keys are the ones you would steal because the public key part is actually public. The private keys that identify people in a public key system are simply strings of numbers that are assigned to people. If one is compromised in any way, shape or form, you simply tell everyone it is no longer any good and you get another one. It is just the same as replacing your keycard from a bank.

Ms PLIBERSEK—Would you necessarily know if your private key was stolen?

Mr Paddon—No, you may not. It very much depends on what the private key is being used for and how it is stored. If a private key is stored in a secure key storage of some sort, then it would probably be like with a smart card—the key storage would actually have to be physically stolen, and you would probably notice that it was gone. If it was simply a file on a disk on a computer, then it is only as secure as the surrounding operating system. If you use a fairly weak desktop operating system, then there are obviously issues that have to be dealt with there. However, the private keys can also be protected by pass phrases, so you can have several layers of protection. Someone may actually steal the file, but they cannot use it without the pass phrase.

Ms PLIBERSEK—Can you take a step back and explain to me how I would use a private key if I had one?

Mr Paddon—The way this works is that you actually create two keys: a private key and a public key. You tell everyone your public key and you keep your private key secret. Using that private key, you can effectively digitally sign documents. Basically, that is information that you can add to the end of a document that only someone with your private key could have generated.

Ms PLIBERSEK—Say that you have written your documents—you are emailing a tender bid off to someone—and you want to sign it electronically. Do you type in a number or do you click and drag a file? How do you actually put the key onto the document?

Mr Paddon—Perhaps a real life example would be good. I use public keys all the time for signing my email. My email program knows all about them. It knows my PGP keys. Every time I send a bit of email, I click 'sign' and it signs it. If I have not actually provided my pass phrase recently, it will ask me for my pass phrase again, which is just an extra level of protection that I

have chosen to add to my usage of public keys. It is that easy; it is completely integrated with whatever software you are using.

Ms PLIBERSEK—Does the person you are sending the email to need any particular software to read that key?

Mr Paddon—Absolutely. The PGP is a good example of a public key system because it is based on a standard Internet RFC standard, so there are many pieces of software. All the Internet standards are called RFC documents. It used to stand for 'request for comment', but they are actually standards documents—that is just a historical thing. Because it is based on a standard, there is in fact a wide selection of software systems which understand that particular sort of digital signature or that particular sort of encryption of an email and therefore can handle it. Most common email programs, for instance, have that capability.

Ms PLIBERSEK—One of the witnesses before the committee yesterday said that they do a lot of business overseas. They were talking about Gatekeeper specifically and they said it made it a little difficult for them because they have a lot of information to transmit and the people that they are dealing with overseas do not necessarily have the appropriate programs and so on to read the encrypted information that they would be sending under that system.

Mr Paddon—That is probably a very good argument for the use of open source so that all parties around the world have equal access to the software.

Ms PLIBERSEK—So when you send the message it says that if you do not have the software you can download it from the Internet by clicking onto this button.

Mr Paddon—Sure; you could certainly do that. PGP emails are so ubiquitous that most people do not bother with that. But if it were something more Gatekeeper oriented, which is an X.509 standard—a different standard—then, yes, you would want to provide people with the software as well as the document itself.

Senator LUNDY—Just on that point, Gatekeeper is one type of PKI but there are many different commercial versions of PKI systems. What are the relative strengths of PGP or open source PKI compared with the more proprietary or commercial products on offer?

Mr Paddon—In the open source world and the commercial world you will find examples of all the different types of approaches, so it is not that the commercial world has approached the problem in one particular way and the open source world has approached it in a different way. For instance, PGP, at least until recently, was available as a commercial product as well as an open source product, and that was the web of trust model. Similarly in the X.509 world.

Senator LUNDY—Can you tell me again what the PGP standard is—that is the RFC?

Mr Paddon—All RFCs have unique numbers. I do not recall the RFC but it is called the open PGP standard. If you went to the Internet and searched for it on Google it would pop up pretty quickly. The X.509 standard is an ISO standard and you could obviously contact Standards Australia or an equivalent body to get a hard copy of that.

Senator LUNDY—Is X.509 a global standard?

Mr Paddon—I regard both of those as global standards. X.509 is a hierarchical tree of trust model, which basically requires certificate authorities to sit at the top of the tree. Generally, a lot of the global certificate authorities see themselves right at the top and then below that are world governments. That may or may not be the way that various governments see that.

Senator LUNDY—Indeed.

Mr Paddon—Of course, there are clearly jurisdictional issues when you are asking someone outside of the country to run your public key infrastructure. X.509 is tree based and requires people at the top of the tree to be trusted by everyone. The web of trust is the competing approach. Both of these approaches are found in open source and commercial products.

Senator LUNDY—I was very interested in your comments earlier about why a government would choose to embark on their own PKI infrastructure, like Gatekeeper, and your observations about what their motivation could be. Is it as simple as governments wanting to be at the top of the tree?

Mr Paddon—There are a number of issues. The reason that one would embark upon hierarchical PKI in the first place is simply one of scale. If you need to distribute a unique public key to every person in the country and then somehow certify that those public keys are what they pretend to be, you need some kind of structure there. That implies that someone in the system has to be ultimately trusted—a third party or arbiter of what key means what and who belongs to which key. It would be a matter of government policy to decide who was trustworthy enough to fulfil that role. Clearly it is a role that could be performed by government directly or it could be outsourced to the commercial world. But if it were outsourced, AUUG feels that the appropriate safeguards and policies would have to be in place for the long term.

Senator LUNDY—I am familiar with the ongoing debate about who sits at the top of the tree and issues about the power of government to decrypt messages sent by PKI. Certainly, in some spheres, concern has been expressed that public key infrastructure managed by government, or if the government has a close enough relationship with the company at the top of the tree, could compromise the data. The pros of this debate are, of course, national security related issues and the cons are the severe invasion of privacy. I am trying to get the committee to get an insight into that debate: whether it is still raging in the community, particularly of Internet users and people who are interested in cryptography, and where it has moved to in the current heightened security environment.

Mr Paddon—That is a relatively complex set of questions. In the cryptography community, everyone is paranoid. They would not trust the commercial side or government. More realistically, I think there is probably generally more trust in governments than in commercial entities because they are probably more answerable in the long run and there are clear mechanisms for a government to be answerable. That will obviously differ from place to place in the world depending on how people view their—

CHAIRMAN—We would think that we are an important part of that.

Mr Paddon—On the intercept side of things, it is important to point out that while public key cryptography can be used to encrypt things, it is more often used as an authenticator. The issues with intercept have to do with more traditional cryptographic techniques. If I wanted to hide something from a law enforcement agency or from the government, I would probably not use a key that I knew was subject to escrow if I had some kind of ulterior motive. I am not sure whether intercept makes a lot of sense when you are worrying about authentication issues. It is a separate issue.

Senator LUNDY—In that case, we will move on. More generally with respect to open source, we have heard various opinions expressed at this committee about the relative merits, as far as security goes, of open source versus proprietary software. Do you have any comments about that? Could you give us the view of the UNIX users group about the ability of open source to be perhaps more secure than at least some versions of proprietary software?

Mr Paddon—I think AUUG contains many opinions about this. In general, we feel that while there is a place for all systems, and while we are all about interoperability, in the recent past—the last 10 years or so—the open source world has demonstrated substantially more security than the proprietary world. We feel this because it is clear that the large proprietary operating system vendors do not make money by making their products more secure. It is not that they do not want to or there is anything wrong with them; they are very good at what they do. However, it is not necessarily good business sense to spend a lot of money on security. For example, how many people would go out and spend another $500 on a new version of Windows just because it was a bit more secure? I would put it to you that that would be a fairly small niche market.

Just because something is open source does not mean that it is secure, but because there have been open source projects that have focused on security as a prime goal, their security record has been much stronger than that of the proprietary world. A very good example is the OpenBSD system, which is an open source project based in Canada. That has probably achieved some of the best security results of any operating system on the market. That is not designed for military use and therefore unusable for anything a normal person would want to use it for. There are similar efforts in the Linux world and so on. Over time you will see that the open source world will tend to produce products that are more secure than the proprietary world until there is a good business case for the proprietary world to do otherwise.

Senator LUNDY—In the interests of clarity, my understanding is the one of the reasons that open source software has a strong claim to being secure—as you say, in some circumstances—is that because users and people with the technical skills to write code have access to the source code, they can continually test it and make improvements to it. They are not prevented from finding potential holes or bugs. That adds to the ability of open source software to be tested in a very challenging using community and not just used with a commercial guarantee or commercial assurances.

Mr Paddon—The issue of access to source means that an enormous amount of peer review goes on. Certainly, not everyone who uses an open source system looks at the source code, but the fact that it is available means that it is looked at by a very broad number of people from different educational and cultural backgrounds, and that diversity leads to a lot of out-of-the-box thinking; therefore a lot of problems are found proactively and are fixed.

What is interesting and rather amusing is that the converse is not true. The fact that you do not have the source does not make something more secure. There have been many examples of this in the desktop world recently, and even in the UNIX world of yesteryear, which were all closed source proprietary systems. People can build tools to probe for various systemic weaknesses—well-known types of weaknesses in software—and do so without the source code being available. In many ways, not having the source is no protection; having the source is a definite bonus for peer review. So, yes, the nature of open source tends to make it more secure.

CHAIRMAN—Microsoft doesn't agree with you.

Mr Paddon—I am sure they wouldn't agree, although I must say that Microsoft has, for instance, agreed to provide its source code to the government of China recently, I believe. I saw that in the news. The reason behind this was exactly what we are talking about.

Senator LUNDY—It was because of security concerns about what was contained in the source code of Microsoft's products, wasn't it?

Mr Paddon—I could not speak for either of the two parties.

Senator LUNDY—I am just working from media reports.

Mr Paddon—Yes.

Senator LUNDY—Because the chairman raised the issue of Microsoft, one of the things we have already heard about is the necessity for patches to be distributed for proprietary software as weaknesses are found. The company hopefully is alerted to those weaknesses before they are exploited; a patch is built; and then it is up to the technical people on the ground to put those patches in place. What is the equivalent process for open source if weaknesses are found? How do they get fixed?

Mr Paddon—I think it is fair to recast the question to when weaknesses are found. Any software is subject to having weaknesses found, regardless of whether it is open source or proprietary. Exactly the same process occurs: the people responsible for the piece of software generate fixes or patches, distribute them and some proportion of the user community applies them. The commercial world—and particularly Microsoft, if I can speak specifically about them—have been getting very much better in the recent past at producing patches in a timely fashion. That has not always been the case. It is of some concern to AUUG that that may not always remain the case. The open source world, because it is a peer review world, tends to have a very quick turnaround time for production of patches, but it is in fact the same sort of mechanism.

Senator LUNDY—What about the distribution of the open source patches?

Mr Paddon—It is distributed in the same way that the original software was distributed—through the same channels, which is usually online.

CHAIRMAN—Can I follow up on that. I am advised that Sendmail handles up to 75 per cent of all email traffic and that in early March the DSD released a computer security advisory

stating that the latest version contained a critical vulnerability. This vulnerability could allow a cracker unrestricted remote access to any system running that version of Sendmail. Are you familiar with that?

Mr Paddon—Absolutely.

CHAIRMAN—Can you tell us about it?

Mr Paddon—Perhaps I can give you some more history. Sendmail is a very interesting case, in regard to both the way open source works and the way security problems arise in online software. Sendmail has been around since at least the early eighties. As a consequence, it has become the de facto mail transport program on the Internet. In that time I would regard it as having had a very large number of security problems. It really comes down to the fact that Sendmail was designed for a completely different, more friendly Internet many years ago.

On the plus side, one can note the people in charge of Sendmail, in particular Eric Allman, who has for the last 20 years or so been extremely proactive, and also very swift when he needed to be reactive, in finding and fixing security holes and publishing patches. I believe that is a very strong track record and one that outstrips any commercial organisation I could name. However, that being the case, AUUG would not necessarily recommend Sendmail as the ideal open source mail transport program. There are many others available, some with exceptional security records, in particular, just off the top of my head, there is an open source mail transport agent called qmail, which in fact has had no security problems for its entire lifetime. It was built as a secure transport from the ground up. It has been widely available for around about a decade.

Ms PLIBERSEK—You were talking about PGP earlier. How does PGP handle the revocation of a compromised identity?

Mr Paddon—With PGP you publicise your public key—there are what are known as public key servers where you can put your key. When you generate your key you can also generate what is known as a revocation. If you ever feel that the key has been compromised or should no longer be used for whatever purpose, you publish a revocation just as you published the original key so that anyone using the key server can see that that key should not be used. The revocation cannot be forged because it is digitally signed so people know who it came from. Did that help?

Senator LUNDY—Is that real time?

Mr Paddon—Yes.

Senator LUNDY—If you put in that revocation, it is there straightaway and there is no delay?

Mr Paddon—That is right, if everyone is using the online system. If people are relying on an offline copy of your keys, they will not become aware of a revocation until they go back online again.

Senator LUNDY—Open source is gaining a great deal of interest around the world at the moment. China is probably a good example of a government that has expressed interest in using open source. Are you able to give the committee some observations about the growing awareness about open source technology around the world and the interest, particularly from governments and indeed big corporates, in this type of software as opposed to commercial proprietary software?

Mr Paddon—Open source is fairly common in the commercial world around the globe. Every Fortune 500 company has a significant amount of open source software in use. Large companies like IBM, for instance, are expending a significant amount of money. Traditional UNIX vendors, such as Sun Microsystems, are moving slowly towards an open source type methodology. Very clearly, it is widely used in the commercial world, and I think it cooperates and coexists very well with proprietary systems you also find. In government, I think it is a little more complicated and a little less clear.

There have been some very outspoken cases, such as Peru, where there have been government ministers making all sorts of noise and commentary about the utility of open source, not only from the perspective of interoperability and freedom from lock-in but also from the perspective of cost to the taxpayer. Clearly, that is a very important issue for government. China have produced their own version of Linux, which I believe they call Red Flag Linux. They have a number of concerns that they have been trying to assuage, and one of them, I believe, is cost and the preservation of their foreign currency reserves, but there is also concern about security. The media has reported that China have evinced some concern about the security of government data and that they wanted to have some degree of control. Other countries such as India and Germany have also been outspoken from time to time, and that has been reported in the media. It is very hard to tell, without actually engaging those governments, exactly as to what is going on inside them, but that is the broad overview.

Senator LUNDY—You mentioned lock-in. That has certainly been an issue of concern with the Australian government and the various arrangements with large vendors. Can you explain what you mean by the concept of lock-in?

Mr Paddon—There are many forms of lock-in but from AUUG's perspective the most dangerous and pernicious form is the proprietary data format lock-in. Using a proprietary system or application of some sort puts you into that situation. The problem with lock-in is that there is no guarantee that a particular commercial organisation is going to remain in business or is going to remain supporting that software for any particular period of time. Certainly in my personal experience I have files that are only 20 years old that I could not read if my life depended on it. One imagines that the sorts of records that the government has to keep properly will need to exist for substantially longer than 20 years. Nothing stops you from systematically converting file formats every time you change applications, but the cumulative cost of such an activity would be mind-boggling.

CHAIRMAN—The Victorian electronic records strategy says that records should be converted into one or more long-term preservation formats to protect them from obsolescence. Are you familiar with that?

Mr Paddon—AUUG would very much agree with that. In fact, we feel that the correct form is probably XML at this point in time.

Ms PLIBERSEK—That is what the National Archives do, isn't it?

Mr Paddon—We are not familiar with exactly what the National Archives do.

Senator LUNDY—The National Archives have not established formally the standard of XML but I understand that the British government has declared XML as being its general standard. The National Archives are looking at in their current strategy. I was going to ask you about that. So you think that is a good format?

Mr Paddon—Absolutely, and I think it is a very natural extension for the government. For instance, I am aware that *Hansard* has for many years been stored in a human readable mark-up format. While that in itself is peculiar to *Hansard*, it is a very small step to XML from there and it is very clearly an approach that has worked for *Hansard* for many years.

Senator LUNDY—I think I read in your submission, and you might be able to clarify this, that you also think that long-term records should be encrypted.

Mr Paddon—Indeed. It depends on the nature of the record. If it is purely a public record, there is no need for encryption. AUUG is concerned about the areas of privacy and confidentiality for records pertaining to citizens in general. Obviously, there are other sorts of documents that the government would wish to protect as well.

Senator LUNDY—Can you encrypt XML?

Mr Paddon—Absolutely.

Senator LUNDY—No problems?

Mr Paddon—No problems whatsoever, with a proviso that if you choose a proprietary encryption mechanism you are back to square one.

Senator LUNDY—In your submission you were talking about the TLS protocol, formerly known as SSL. Can you tell me a little bit more about that and its role?

Mr Paddon—Yes. We foresee that online access to government records is going to become more and more the norm. As for the records themselves, the data may be well protected in a central high-security facility with great security policies and all the right software but, if people are accessing it from the outside, the chain is only as good as the weakest link and it is very important if people are coming in, in an online sense, that their authentication be done properly and that the data be encrypted while it is in transit so that it cannot be intercepted or modified. As a consequence, there are good standard protocols, such as TLS, that we feel are appropriate to the task. We feel TLS is the minimum level of security that one would want to aspire to.

Senator LUNDY—Other witnesses have talked about SSL as their chosen security option. Is TLS the standard that SSL complies with?

Mr Paddon—Yes. SSL was never actually a standard; it was just something put together by a company called Netscape many years ago. But TLS is an extension of SSL which has been standardised as an Internet RFC.

Senator LUNDY—Is that open source?

Mr Paddon—Standard is not open source per se because it is not an implementation.

Senator LUNDY—But SSL as a solution is, isn't it?

Mr Paddon—Absolutely. There are open source implementations freely available. I might add that it is supported by pretty much every browser on the planet, which makes it a particularly handy protocol to use.

Senator LUNDY—Yes; you see it a lot. What would the scenario be if something like SSL was proprietary? If companies wanted to create that secure sockets layer with their clients or customers, how would it work if it were proprietary and not an open source solution?

Mr Paddon—This is quite interesting. Allow me to propose a gedanken experiment for a moment. Imagine that you had a government web site that only supported a particular browser that was available from only one vendor—and that would be exactly the same as only supporting SSL from one vendor. You would find that the information would only be accessible to those people who had bought the appropriate software from that vendor. If you were using that sort of technology to provide service to the citizenry as a whole, you would be mandating it: they would all have to spend their money on a particular software package from a particular commercial vendor. That would be the consequence of proprietary implementation.

Senator LUNDY—That would create a huge market gift.

CHAIRMAN—I think we did something like that back in the early nineties with respect to online purchasing systems.

Senator LUNDY—Perhaps you should talk to the tax department about what they are doing at the moment, Mr Chairman.

CHAIRMAN—We did something like that. It was to give broad access across the whole scope, but it was very expensive for people to join up.

Mr Paddon—AUUG feels that situations like that promote monopolies and that, in general, monopolies are not necessarily desirable.

Senator LUNDY—In terms of the sheer market coverage and market power that Microsoft have, there has obviously been an increase in their market share in government contracts recently. Do you think that there is a place for government policy to guard against the development of a ubiquitous proprietary software product, particularly when it is about interaction with citizens?

Mr Paddon—AUUG's position is that it would hope that the government would make the best technology choice at every juncture. Sometimes the best technology choice may indeed be a proprietary system. It may provide features, capabilities or some functionality that is only available with that system. However, AUUG feels that the government should seriously consider using open systems, particularly where equivalent functionality is available at a much lower cost and with all the benefits of open source software.

CHAIRMAN—Thank you very much. We appreciate your time. By the way, what does AUUG stand for?

Mr Paddon—It actually stands for nothing officially, but historically it stood for the Australian UNIX Users Group.

[11.45 a.m.]

BEZZINA, Mr Mark, Director, Business Standards, Management and Business Communications, IT and eCommerce, Standards Australia International Ltd

NAVARATNAM, Mr Panjan, Projects Manager, Communications, IT and eCommerce, Standards Australia International Ltd

CHAIRMAN—Welcome. We have received your submission, for which we thank you. Do you wish to make a brief opening statement or should we go straight to questions?

Mr Bezzina—I would like to make a very brief opening statement, just to thank the chairman and the distinguished members of this committee for giving Standards Australia the opportunity to present.

CHAIRMAN—It is a pleasure. You will think this question is a bit sarcastic, but outside of being expensive and voluminous, which as a former user is how I found them, what role do standards play in the management and the integrity of the Commonwealth's electronic data?

Mr Bezzina—Could you explain what you mean by 'expensive'?

CHAIRMAN—As a building contractor, in order to satisfy a number of contracts I sign, particularly those for the state government of Victoria and/or the Commonwealth government, throughout the specifications they require you to adhere to certain standards by number. That means you have to go and buy the things and put them on the shelf.

Senator LUNDY—In order to comply with the law.

CHAIRMAN—Absolutely. In order to comply with the contract which you had signed. It meant we had bookshelves full of standards which we rarely needed to refer to and they were expensive.

Mr Bezzina—Thank you for that clarification.

CHAIRMAN—So you would understand the direction I am coming from.

Mr Bezzina—In justification of our business model, Standards Australia plays the role of facilitator. We have to be very careful how we operate. We have to operate in a way that equally advantages or disadvantages everybody in the committee process. We have to be funded through the sale of our products, as unfortunate as that is. That methodology gives us the freedom to be genuinely open to all points of view. Standards Australia operates through a series of committees and it is not a cheap process getting a bunch of people together and allowing their input, providing a secretariat, audio and teleconferencing facilities and the like. That is pretty much the nature of what we do, even to the extent of taking minutes of meetings. In addition to that, we publish about 9,000 standards and we will make some money out of about 100 of them. The whole market for the rest is the committee and they get a free copy anyway.

Ms PLIBERSEK—That was a pretty good answer.

CHAIRMAN—I must have had to buy the 100. Leaving the sarcastic bit aside, what role do you have to play in the integrity of the Commonwealth's electronic data?

Mr Bezzina—We have a very important role to play in that we bring communities together in way that gives everybody an equal say in how things are agreed upon, and that forms the basis of the committee. Committees are constituted through national nominating organisations and they represent broad stakeholder perspectives. We have done a lot of good work in the area of information management and information security. We acted as the secretariat to Project Gatekeeper. I noticed NOIE representatives were here earlier. They may have mentioned some of our joint projects on ebXML, setting up a national registry and framework for electronic messaging within Australia. We have done work on records management, knowledge management, risk management, corporate governance, IT governance, cyberforensics, biometrics—and I could go on. We have 1,500 committees, 9,000 committee members, 1,500 nominating organisations and we publish 500 standards a year.

We are process driven, but we have to be. The areas I manage are communications IT and e-business standards and management of business standards. The development of those standards is completely different from standards that have gone before them in that the traditional approach to standardisation was to just document what was done within an industry. It was a fairly simple process. The next stage was when industry was doing similar sorts of things but there was a need for consensus. You had to get the parties together and get them to agree on what the right way forward was. Now we are in a technology based environment, the standard quite often sets the industry up. So you are at the front end of how things are going to operate. You are an enabler for an industry, whether that be XML or data communications or a whole series of other things, such as information security.

It was interesting to hear the gentleman from the Australian UNIX user group give a perspective on information security. As a component of the important area of data management, that perspective was just a small piece of the picture. You mentioned somebody pinching your key, and that is a real problem. So you do need to have biometrics or some sort of fail-safe method of identification at the beginning of the chain. You need to have encryption methods for identification and then revocation methodologies. You need the public key infrastructure there, but that is only part of it, and then there is the security of information, the encryption of that information, as it passes through from a sender to a receiver. Once the receiver receives the information, that information then has to be stored somewhere, and it has to be stored in a way that is not compromised for evidence purposes. So we have done forensic standards, we have done biometric standards, data interchange and communication standards. Once that information is stored, it is acted upon. If the information is in a form whereby it cannot be acted upon, it requires a human interface. So registries all of a sudden are important, and being able to access data out of those registries using metadata tags is an important component. We have done a lot of work with the AGLS standards, but also with the ebXML registry with NOIE.

Senator LUNDY—What is the difference between ebXML and XML?

Mr Bezzina—XML is just the native mark-up language so that you can define data structures as opposed to the old-fashioned HTML, which was really about presentation. ebXML is a whole framework for conducting electronic business and includes data—

Senator LUNDY—Is it actually a language that varies from XML?

Mr Bezzina—XML is at the height of ebXML. It does not actually tell you how to use XML. XML is a standard in its own right. Standards are like an onion, and at the heart of that onion is XML. In its own native form it is not much use to anybody because if everybody is going away defining their own tags for data interchange, then you cannot communicate. So XML puts a framework around it and says that if you are going to develop messages for exchange and data storage, what you should do is have a methodology for defining those tags in a consistent way. If you have data elements such as name and address, if people in different pools all over the world or in a nation are developing messages, they use those core components.

Senator LUNDY—So the 'eb' is that extra bit?

Mr Bezzina—Electronic business, yes.

Senator LUNDY—It is very important.

Mr Bezzina—It is an important distinction.

Senator LUNDY—Please continue.

Mr Bezzina—It is an interesting area. It is like a big elephant. A lot of people look at the tail of the elephant, the tusk, the trunk or the ear. You really have to look at this stuff in perspective. We are in an ideal position to do that. Just in my small area we have 2,000 people that we interact with on committees, and other stakeholders outside that. They come to us and ask these questions. They say, 'We want to do electronic business,' 'We want to store data,' or 'We want to exchange information in a format that keeps it secure.' Then they expect us to give them the answer. So what standard do we use?

Senator LUNDY—Your submission states:

Standards Australia ... (NOIE), and an industry working group will promote the establishment of an Australian ebXML ... registry of standard message formats and business processes for conducting business over the Internet.

What is the delay in declaring and publishing that standard and having it out there?

Mr Bezzina—That is a good question. What we are trying to do is more than just identify it but bring industry with us. At the moment you have the health industry doing their own thing within Standards Australia, you have the meat industry, the hardware industry, the telecommunications industry, the super industry and a lot of other industries currently working on developing electronic messages and structures. It is not a technical problem—none of this stuff is a technical problem; it is a social problem, and it is a problem of buying into an approach that people can live with to develop messages. That is where the hold-up is. We can use the technology and it is very easy to put the bits and pieces together within the first six

months of the project. We have already developed a registry that would suit the needs of all those stakeholders, but getting them to agree on a methodology for a national messaging framework and then getting a critical mass around it is the difficult step.

Senator LUNDY—Because XML is so ubiquitous and other governments have mandated its use as the standard format, is the eb part of XML a global movement in its own right or is it being developed in Australia? What potential does it have to change the nature of what you describe as the core of the onion? Does it add elements to XML that become peculiar to Australia and Australian industries and departments, for example?

Mr Bezzina—It is an international initiative under the UN/CEFACT banner. It is a joint initiative with OASIS, the Organisation for the Advancement of Structured Information Systems.

Senator LUNDY—Is that under an OECD or UN banner or something like that?

Mr Bezzina—OASIS tends to be a vendor driven forum, but UN/CEFACT is under the UN banner, and they traditionally did the EDI type standards. We are not trying to pick standards. Web Services is another component that is increasing in popularity. What we are trying to do is to say, 'What is a framework that will work?' There are bits and pieces that work and there are bits and pieces that will not work, so somebody has to do the homework and say, 'What bits can we take now?' People have a real need now to—

Senator LUNDY—You could just take XML now and then keep talking about the eb part of it, couldn't you?

Mr Bezzina—You cannot, because when you go to exchange information the semantics of the message are different. How you define a name and address or how you use the meta tags within XML to exchange information are different. If you go from a message methodology, you basically map out what your existing relation is with your suppliers.

Senator LUNDY—How did the UK government declare XML as a standard? Did they resolve these messaging issues on another layer or on top of that?

Mr Bezzina—That is a hard question. You can define XML, but that is the middle layer of the onion; it does not really do anything for you at that stage in declaring XML, because XML can have many different strands. In the electrical industry they have aseXML, which is an application of XML but tailored for the electrical industry for their market operations and Ebco, the Gas Market Company and those sorts of organisations, but the problem is that when the electrical industry or the energy industry try to talk with government or try to talk with their supply line providers they run into strife. Then it means redoing everything they have already done.

Senator LUNDY—How can you ensure that ebXML is non-proprietary?

Mr Bezzina—By its nature. But ebXML is not the answer. Web Services is not the answer. It is saying, 'What bits of that can we use in a way that doesn't lock us into the future?' You focus on a methodology that will be portable between operations and take the best bits. Web Services

is very good for serving up information in XML format, but then ebXML have collaborative partner profiles and collaborative partner agreements, which is a very important area in business. Essentially, they are saying, 'Here's how we operate.' It is like a combination of white, yellow and green pages. You are familiar with the white and yellow, but the green pages are the capability in electronic form for, say, Coles Myer wanting to interact with the sponge supplier. That can be an automated agreement but Web Services does not provide that functionality, so you use that functionality from ebXML. You might use the XML methodology in terms of the registry, but then you may use Web Services as an interface because that is becoming a widely used type of service, just because that is the practical way of doing things at this time, as long as it does not lock you in for the long term.

CHAIRMAN—If you do not want to lock into the long term, what do you have as a standard for long-term data storage?

Mr Bezzina—XML is an excellent framework but how you go about defining XML—

CHAIRMAN—You keep changing the operating systems all the time and 30 years from now those systems may not be around.

Mr Bezzina—But it does not matter. If it is in XML, then that is fine but you have to be careful about how you define XML. XML is very simple. In the old-fashioned days if printers had bold on a heading, then it had 'bold' on either side of it. That is all XML is about, and you define the terms such as 'bold'. It tells you how to store information so all the bold things will go with all the bold things and all the—

CHAIRMAN—That is fine but what about being able to read it 30 years down the track?

Mr Bezzina—It is human readable and it is machine readable. The problem is where people use 'bold 1' and other people use 'bold' and what the format is of the character set that goes within that bold that gives it a code. If '1' means bold, you have trouble. But if you set up a methodology for defining processes and also a methodology for the core components of the messages once they are constructed, that makes it achievable to do what you are saying in having a timely record set that can be read by any application.

CHAIRMAN—Punch cards are still readable but who has a punch card reader?

Mr Bezzina—This is different. I agree with what you are saying. That is an interface issue.

CHAIRMAN—That is the way the data was held; the data was stored in punch card form. So if I go back 30 years and I find a deck of punch cards and I want to know what the data is, I am going to play holy hell in trying to read it. I can store it, but who has a punch card reader anymore and what is it connected to?

Mr Bezzina—That is right. The interface point is an issue and how you store the data is an issue.

CHAIRMAN—That is why I am asking about Standards Australia's standard for data storage.

Ms PLIBERSEK—Isn't that what the Archives people were talking about yesterday with the development of Xanadu, which was going to be their—

Mr Bezzina—I have not heard of that one.

CHAIRMAN—It sounds like an African disease!

Ms PLIBERSEK—They are working on an interface.

Senator LUNDY—I cannot recall exactly what Xanadu did—

Ms PLIBERSEK—It reads XML. It is an interface.

CHAIRMAN—That is storage regardless of the software used to record it in the first place.

Ms PLIBERSEK—They were trying to create, using some software, a system of reading materials stored in the most basic format of language, which is XML. The software was trying to do it in a way that was not reliant on any proprietary elements that may have been involved in the creation of the XML in the first place, so it had stripped back any surplus code in that data and enabled it to be read.

Mr Bezzina—That is an important development but also, as the chairman says, even disks are going to be a thing of the past, hence all that data you have stored on your little floppy disks—

Ms PLIBERSEK—They are in our laptops now, aren't they? You can actually put in a floppy disk reader as an attachment but they have only got—

Senator LUNDY—CD-ROMs.

Mr Bezzina—That is right. That has become an issue with regard to all the disks you have lying around the house. It is an important point, but we do not go to the level of defining it. We have committees that look at the magnetic storage of data at the ISO level under JTC1.

CHAIRMAN—So all you are concerned with is the basic format of the data, not the mechanics of what it is held in.

Mr Bezzina—That is right. We do define those types of storage medium, but we would say that the users must choose what is appropriate for them. So a punch card may be useful for inputting information at a point in time or a small disk drive may be useful, but the user has to determine whether storing it in that fashion or storing it on a commercial strength database—

CHAIRMAN—We used to store it on tape decks.

Mr Bezzina—Yes, and there was the same problem again.

CHAIRMAN—We stored it on punch cards to begin with and then we stored it on tape decks. We would have a hell of a time reading those today, too, I suspect.

Mr Bezzina—You would be right, yes.

Senator LUNDY—I don't think it is useful to oversimplify it. Data is updated as you go. There is data stored now that I am sure has had its troubles with being updated and being backward compatible and all the rest of it.

CHAIRMAN—I am just interested in the storage question.

Senator LUNDY—It begs the issue of proprietary storage systems as well and the operating systems in which—

CHAIRMAN—I never thought about it before until we started this inquiry, but now I think about it.

Senator LUNDY—the open standard data is actually stored. Does Standards Australia get involved in that?

Mr Bezzina—We are looking at this registry but we would have some sort of commercial strength database behind that which would allow mass conversion of the data in a format that would be readable by the greatest number of applications being developed and easily converted. The beauty of XML is that you can develop a style sheet to put it into any form you want. So, provided that data is held in the same sort of format—and that is what you tend to do—you can convert it in a way that presents well in printed form or in a way that presents well on a screen or in a way that presents well for machine-to-machine communication. It depends on your use for it. That is the beauty of XML because you have so much flexibility in how you style it to serve it up.

Senator LUNDY—I know Standards Australia has a very complex network of its own in terms of industry consultation and industry committees where you talk with different vendors. How do you balance the interests of proprietary software companies in these matters and those of the open source movement, given that the open source movement tends not to have vast resources focused specifically on ensuring that Australian standards suit their product, as the proprietary software companies have? How do you balance those competing pressures?

Mr Bezzina—It is a good point. What we see in Australian committees, which is different from committees anywhere else in the world, is a very strong user representation. The US and other countries tend to have a very strong vendor representation. It is interesting that what we develop here is quite often very useful internationally because it is very much focused on the users' point of view rather than on the vendors' point of view—using their market strength and whatever means are available to them to try to influence the outcome. Also, we do have very strict consultation processes and we balance committees. We actually review the constitution of committees. If any particular interest looks like it is getting more air time than the others, then we rebalance it. I like to think of them as forums for conflict because people get in there and they will argue about these points, but in such a way that no single interest group can dominate. That is one of our processes. We have a number of others. We have shorter cycle time processes. As I said, with technology type standards, we are often leading the industry. So within a very short period of time we have to get something out very quickly.

Senator LUNDY—It means you have to be quite brave, too, with technology because it does move so fast. Does that mean that you tend not to do something rather than do it because of the fast pace or do you find that, as you say, it just shortens your time frames and means that you perhaps push out standards faster but perhaps modify them faster as well?

Mr Bezzina—Definitely. It means we push the standards out much quicker and we process them. We provide higher levels of international input to try to influence those outcomes so they meet Australian needs. It means that our cycle time is shortened. As I said before, the standards are an enabler for the industry. You cannot have interoperability until you agree on what the standard is for interoperability.

Senator LUNDY—Do you find that you get hamstrung by international events or perhaps the international time cycles as they get caught up in various forums? Does that have a hindering effect on or perhaps adds a nervousness quota to your decision making? For example, you are about to make a decision but you hold off because they are about to make a decision in an international forum, they then change their mind but you are six months down the track already. Do you know the sort of scene I am talking about?

Mr Bezzina—It is an interesting point. We see quite often that Australia is unique in that we have very good technical capability here, we have very good people, very intelligent people, but at the same time we are not like the US where there is a highly fragmented set of industries. We can essentially get all the key stakeholders in one room—the DSD, the Federal Police and the states and territories—and agree on an approach. That approach, which is developed for a small but commercial-strength country, can be transplanted in the US.

Senator LUNDY—Do we punch above our weight in the international standards forums?

Mr Bezzina—Definitely, and we hear that very often. We are also seen as a neutral arbitrator between the US and Europe.

Senator LUNDY—It is a very important role that you play.

Mr Bezzina—That is right. We are in a key influencing role.

CHAIRMAN—Could you get them to agree on metrics or otherwise?

Mr Bezzina—We pick our battles!

Senator LUNDY—Let us talk about privacy for a minute. What role do you play in privacy standards—for example, with the National Privacy Principles? Has any of that legislated base been transferred directly into standards that you have been able to take into international fora?

Mr Bezzina—In terms of taking them into international fora, not so much—and most of our privacy principles are derived directly from the OECD principles anyway so there is not a huge difference. Privacy is a small part of the picture as well. To have privacy you need security, and security is a big question mark at the moment.

Senator LUNDY—They certainly go hand in hand.

Mr Bezzina—We have done a lot of work on information security management systems which provide a broad structural approach to managing security, and that has been picked up by the Defence Signals Directory in their ACSI 33 document. Great slabs of that document now refer to our information security standard. In its annex, that standard used to have the National Privacy Principles, but we took those out and just made reference to the Privacy Commissioner's web site because the legislation has changed around that area as well.

Senator LUNDY—Was that taken out because there is now legislation covering off those issues?

Mr Bezzina—Yes. We tend not to duplicate what is in legislation with standards; we tend to point to it. Also, we have done application guides to the Privacy Principles for the health industry, and things along those lines. We see ourselves as independent facilitators, so if a group of people come to us with a strong argument to do a particular bit of work then we will engage in that work.

Senator LUNDY—Questions about the DSD's relative autonomy in standard setting have been raised—I think by me. You say that your standards fit into the DSD's security requirements, yet you are the organisation with the industry consultation networks and structures. What involvement does the DSD have at their level in engaging not just with industry but with stakeholders of a particular issue?

Mr Bezzina—It is a good question. I am not sure what consultation they have with their own communities but they are quite often involved in our communities, and that is probably why they could see the value of integrating our standard into their guide. They were essentially duplicating what was in there, and now they reference it and also our 4360 guidelines for risk management. We also have another document called HB231 about risk management in information security, which is a very important area. If you do not get the risks right you cannot get the solutions right. I do not know what methods they use for consultation.

Senator LUNDY—But you obviously have a pretty close relationship.

Mr Bezzina—We have a lot of stakeholders. They are one of many. The amount of people that we have to deal with on a daily basis is incredible. I probably meet about 10 people a week in one-to-one meetings to discuss these issues.

CHAIRMAN—It is a good thing that you have a good memory.

Mr Bezzina—It gets better the more I use it. I struggle to remember some things.

CHAIRMAN—Thank you very much for coming. If we have any further questions, do you mind if we put them in writing?

Mr Bezzina—Of course not, Mr Chairman. Thank you for the opportunity to appear here today.

Proceedings suspended from 12.15 p.m. to 2.02 p.m.

FERGUSON, Mr Robert Scott, Regional Director, Check Point Software Technologies (Australia) Pty Ltd

HURT, Mr Andrew Bruce Mostyn, Consultant, Check Point Software Technologies (Australia) Pty Ltd

LOVEDAY, Mr Jason, Systems Engineer, Check Point Software Technologies (Australia) Pty Ltd

CHAIRMAN—Welcome. Do you have any comment to make on the capacity in which you appear?

Mr Ferguson—I have responsibility for our business here in Australia, New Zealand and the Pacific.

CHAIRMAN—We have received your submission, for which we thank you. Do you have a brief opening statement that you would like to make?

Mr Ferguson—Yes, I do.

CHAIRMAN—Could you make it very brief, please?

Mr Ferguson—I will. The first thing I would like to do is thank you for the opportunity to submit a paper and for inviting us along here to give evidence at this hearing. We congratulate the Commonwealth government on leading this initiative to proactively investigate the issues surrounding the integrity and security of its information asset.

CHAIRMAN—Could I correct you slightly: the government has not called this inquiry; this committee has.

Mr Ferguson—I am sorry.

Senator LUNDY—He is defending his opposition colleagues on the committee.

CHAIRMAN—Absolutely. We are not the government; we are a statutory independent committee.

Mr Ferguson—Check Point's business is about protecting information in electronic assets. It is the only thing we do. We are an Israeli based security software company with offices around the world. This year we celebrate our 10th birthday. The relevance and significance of that is that we have grown up throughout the whole Internet revolution. So we have been able to focus 100 per cent on security technologies as the technology has developed. Businesses and governments around the world are extending their activities and really starting to use the Internet. Our view is that it has not really started to be used fully yet. The Internet, by definition, is a public, open environment. Securing information becomes even more important as more and

more services and information are made available in the public domain, and as more and more information is made available online.

We are global market leaders in firewall and virtual private networking technologies—global leaders in any way that anyone cares to measure, whether it is by revenue or installed base number of licences. Our position in Australia reflects that global leadership. The team here today consists of myself, as the business leader for Check Point; Andy Hurt, who is an independent consultant who works with us to make sure that we do not get too involved in the technology and keeps us very focused on the business application rather than just on the technology that we produce; and Jason Loveday, who is here because he is our key technology expert, focusing on federal government and defence.

We have compiled our submission document based not on technology but on best practices and security strategies. We deliberately did not look at technologies since our strong belief is that the technology is very much second rate to the development of the organisational security culture and the management policies that surround that. We think that the development and implementation of security policies is not a one-off event. It is a living process and one that needs to be ever challenged and ever changing in line with business practice.

We define the threats to Commonwealth government information assets in six very specific categories: malicious acts, being techno crime and techno vandalism; individuals or organisations accessing information to deliberately destroy it or to gain fiscal advantage from it; negligence; human error; systems failure; and environmental challenges—freaks of nature, storms causing networks to come down and that kind of thing.

As the Commonwealth government starts to rely more and more on the Internet as a communications medium and as more and more information sources are created and added, we think that the threats to the integrity of the government's information asset will increase exponentially. We think that a process of evaluation, threat assessment, the updating of security policies and procedures is the only way that these threats can be minimised.

We firmly believe that it is absolutely necessary to establish and design a security life cycle, involving the following key areas. The first one is perimeter protection. What we mean by that is protecting the access point to a network, whether that be something as simple as a dial-up modem, a router or any other piece of technology that is used to access the network where the information is stored. The second one is an ongoing risk assessment. This is not a technology issue; this is a management issue. The third one is the formation and continual review of departmental security policies. The fourth aspect is ongoing penetration testing. By that we mean testing the whole of the environment. It is not penetration testing from a technology perspective, trying to hack into a network; it is testing the integrity of the policies, of the management, of the whole process around which security is applied.

I have a very strong view, based on many years experience in the market and with the technology, and having seen organisations struggle to implement well-managed security systems, that this task—the creation of the perimeter protection, risk assessment, the policies and penetration testing—needs to be undertaken before any acquisition of technology takes place. The technology is absolutely secondary to the process. We are pleased and proud to be

part of this inquiry and we are very happy to answer questions around the technology, industry practices and anything else that is covered in the submission.

CHAIRMAN—Thank you for that. How many people do you have in Australia?

Mr Ferguson—Thirteen.

CHAIRMAN—You downplayed technology versus the significance of security and integrity. How on earth do you guarantee security and integrity if you cannot identify who is playing? If technology does not have a role to play in that, then I am terribly confused. How do I identify you in an electronic environment if I do not have the technology to guarantee that you are you, not somebody else?

Mr Ferguson—It is not so much that we think the technology is insignificant; we think the technology is very significant, and I am very happy to talk about technology. But if it is deployed without the benefit and umbrella of appropriate management processes and best practices, the significance of the technology and the ability for it to do its job are significantly reduced. Let me give you an example, if I may. The tactical deployment of a firewall without appropriate security practices and culture within a company is nothing more than the tactical deployment of a firewall. It does not necessarily protect the information against attacks, and nor does it necessarily protect the right information. So there is a whole process of risk assessment and of understanding which are the valuable assets that have to be protected that needs to come into play before a piece of technology is deployed.

CHAIRMAN—I hear you, but—

Senator LUNDY—Can I suggest you explain it in terms of opening and closing ports on a server protected by a firewall is an example of having a firewall in place, but if all the ports are still open then it does not actually serve the same purpose.

Mr Ferguson—No, it does not serve the same purpose.

Senator LUNDY—So you can have a firewall in place and you can have all the ports on the server open, giving plenty of opportunities for attack, but you can also make a management decision to close off all the additional ports except for the absolutely necessary ones, and that limits the channel in for an attack. Your firewall will still provide protection but you narrow the pathways through which an attack could come. I am just trying to help give an illustration of having a firewall but also having the management practices associated with the firewall, which is a step.

Mr Ferguson—By creating the policies that are applied in the firewall based on traffic usage and on levels of access, if you go through that process first then the application of the firewall to the security of the network is substantially enhanced. By simply putting a firewall in and saying, 'This bunch of people can only access those ports and we don't want traffic from this source,' it is a deployment of a firewall but it does not really build the level of security that a primary asset should have.

CHAIRMAN—If I have this terrific system and the firewall is built up and I have decided how the system is designed, and if I am using my drivers licence as the identification medium, it seems I do not really have much security. There are a lot of people wandering around with false drivers licences.

Mr Ferguson—Again, I come back to this really being a function, from a management perspective, of identifying the key assets that need to be protected. The drivers licence is a good example of authentication. Is that an appropriate level of authentication for the kind of asset that you are trying to protect or do you want to move to something like a biometric device that reads an iris or a fingerprint or—

CHAIRMAN—Now you are defining technology, and that is what you said you were not going to do. I just make that point.

Mr Ferguson—But the definition of technology comes from the assessment of the value of the asset and the risk to the business of the integrity of the asset being corrupted.

Ms PLIBERSEK—Essentially, are you saying you need to make policy decisions before you go out and start spending money?

Mr Ferguson—I think so.

CHAIRMAN—But what is the sense in having a policy if there is no technology that will allow you to implement the policy?

Mr Hurt—The whole purpose here is to create a cycle. There is a starting point where somebody actually starts this process, and there is a continual refinement and growth of the technology. Therefore technology is implemented through the process but it is a continual cycle of reassessment of whether we need more technology or less technology, depending on the policies that are being stated.

CHAIRMAN—Let us assume the Commonwealth government comes up with a policy which says that we will implement a key and then we will turn around and use Gatekeeper as the technology to implement the policy. There are other technologies that you could use to implement the policy, but isn't the technology that you commit to critical to the outcome of being able to satisfy your policy requirements?

Mr Ferguson—If you do not form the management policy in the first place, you never get to the position where you have to make a compromise. One of the interesting things about the technology is that you can have almost whatever you want providing you have an unlimited budget.

Ms PLIBERSEK—And you can put up with the inconvenience of having multiple levels of security.

CHAIRMAN—I am not convinced of that; I am not convinced that we have come up with any technology that is a 100 per cent guarantor of identity.

Ms PLIBERSEK—DNA testing is.

CHAIRMAN—Is that 100 per cent?

Ms PLIBERSEK—Yes, as long as you have a big enough sample, but it need only be a fingernail or a hair.

Senator LUNDY—You are splitting hairs.

Ms PLIBERSEK—You could take half of that hair that he has split and get a good DNA reading.

Mr Ferguson—You can clearly take it to extremes, but I think our absolute position is that without some clear management guidance it is very difficult to implement technology effectively.

Ms PLIBERSEK—That is what our departments were saying yesterday. They have made a variety of decisions based on their varying needs and it is no good having a uniform set of technology because not every department needs that level of security. That is the point you are making.

Senator LUNDY—PKI, for example.

Mr Ferguson—Yes.

CHAIRMAN—Are you familiar with the document produced late last year called *Australian government use of information and communications technology: a new governance and investment framework*, which was put out by the management advisory committee as their report No. 2?

Mr Ferguson—I did see a copy of that which I think I sourced from NOIE. I would have done no more than skim read it.

CHAIRMAN—Considering your interest in the framework, would you make it your business to source a copy, read it and advise this committee what you think about it as a strategy document?

Mr Ferguson—Certainly.

CHAIRMAN—That is not a government publication per se; it is not a political publication, it is a publication by the Public Service. You talked about the number of potential risks to information assets, including malicious acts, negligence, human error, system failure and environmental risks. Which is the greatest potential threat?

Mr Ferguson—The greatest potential threat is usually human error or human risk.

CHAIRMAN—Is that identification again?

Mr Ferguson—It is like any part of a business. The biggest challenge any business faces is employing people and driving and directing them within a culture that, as a manager, you want to create, and with common goals and objectives. That is why we continue to take this very strong position that you have to have in place the process and the culture that focuses on what needs to be secured and the processes around it before you get to technology.

CHAIRMAN—Okay. But if the systems are in place and somebody decides that they want to play games and disrupt the whole of government approach in using the Internet to do business, and if we do not find out very quickly that that is what they are doing, they can shut us down and we might as well not even have a strategy. Is that true?

Mr Ferguson—That is true. So then most certainly some technology comes into place.

CHAIRMAN—I was not talking about technology; I was talking about malicious acts perhaps being the most significant.

Mr Ferguson—If there is not an appropriate management policy and if there is not appropriate technology deployed then, for sure, the government is significantly exposed. In fact we had a discussion earlier today about a real life incident where a professor who prepared a paper towards a PhD—this actually happened in Tel Aviv—was connected to the Internet across the DSL line. Somebody simply hacked into her PC and destroyed the whole of her PhD paper. She had not kept a back-up. She had a friend in Check Point and she said, 'Come and have a look at this.' He took some friends, had a look and said, 'For sure, you've been hacked.' Somebody had just come in, not necessarily intending to be malicious but with the result being malicious and significant. Anyone who is connected to the Internet in any way, shape or form needs the appropriate level of security that manages traffic coming in and out. That is the starting point and that is what we talked about as being part of that first step: ensuring that perimeter protection is in place.

CHAIRMAN—Have you examined Gatekeeper?

Mr Ferguson—We know Gatekeeper.

CHAIRMAN—What do you think of it?

Mr Ferguson—I have to take a very biased view and say that we at Check Point have absolutely the best perimeter protection available on the market. That is borne out by our market leadership.

CHAIRMAN—So you are better than Gatekeeper?

Mr Ferguson—I believe so. I can tell you from a technology perspective that it goes down to—

CHAIRMAN—Open source or closed source?

Mr Ferguson—We are very much a supporter of an open security environment and as such—

CHAIRMAN—But your system is closed. If I want to use it I have to pay for it.

Mr Ferguson—You have to pay for it if you want to use it—absolutely.

Senator LUNDY—Is it based on open source software or is it proprietary?

Mr Ferguson—It is a proprietary environment but what we do have is a series of published APIs, or application programming interfaces, so that other software can be integrated within the Check Point platform.

Ms PLIBERSEK—You talk about key information security risk analyses that should be done yearly. Do people hire you to come in and do one of them?

Mr Ferguson—People hire our business partners to come and do that sort of thing.

Ms PLIBERSEK—And then you help them upgrade when the weaknesses are found?

Mr Ferguson—Absolutely.

Ms PLIBERSEK—What does it involve?

Mr Ferguson—The level of involvement varies from company to company, but principally it involves implementing some best practices that enable an organisation or a company to identify and evaluate their information assets and therefore have some mechanism by which they can prioritise how they go about protecting them.

Ms PLIBERSEK—There are quite a number of standards that apply across government departments. Do you think that those standards are adequate?

Mr Ferguson—We live in a world that evolves and evolves very quickly, so they are only as adequate as the review process that is in place to ensure that they are in line with changing threats and changing circumstances.

Ms PLIBERSEK—They are only adequate until someone cracks the code.

Mr Ferguson—Yes.

Ms PLIBERSEK—When you are doing a key information security risk analysis for an organisation and a company, what are the factors that you look at?

Mr Ferguson—You break the information assets down and you evaluate them in terms of: 'This is critical information to the operation of our organisation. This is peripheral. This gives us legal exposure if it gets into the market,' and so on. The first thing to do is to understand the asset list. This is why senior management have to be involved in this whole process, because they are the only individuals who can take a holistic view.

So the first thing to do is to evaluate what you have got and what you need to protect. The second thing to look at is where it is going to go and who you are going to give access to, as

well as what potentially they are likely to do with it. The next thing to do is to really look at an evolving review process of the decisions that you make; then you can start to build a life cycle. So if you have identified what is important and you have identified who the key stakeholders are, you can then start to evaluate and build a life cycle process around which you review and look at that.

Ms PLIBERSEK—Do you mean the life cycle of the equipment or the life cycle of the information?

Mr Ferguson—I mean the life cycle of the information.

Ms PLIBERSEK—But there comes a day when you do not need the information anymore, so it is a matter of how you are going to store it securely.

Mr Ferguson—That is right, or remove it totally. Then you start to look at technology. So once you have that firmly established, once you have some value and some process in place, you can start to look at the technology that you apply to it.

Ms PLIBERSEK—What you seemed to be saying at the beginning was that a security culture in an organisation is just as important as the equipment itself. Does this risk analysis look at the security culture of the organisation as well?

Mr Ferguson—Yes. The security culture is about how you authenticate. It is about individuals within a company or an organisation understanding the importance of passwords and logging off and how to utilise the technology.

Ms PLIBERSEK—With most of the organisations you deal with, is the gap more at the security culture end of the spectrum or is the gap more likely to be at the technology end of the spectrum?

Mr Ferguson—More at the management and culture end.

Ms PLIBERSEK—Do you think that is because people are not aware of the potential for disaster?

Mr Ferguson—I think that is part of it. I think that we, as corporate bodies and as government organisations, still have a lot of maturing to do—not in understanding the technology in detail but in understanding the application of technology and why, from a management perspective, you would want to put it in place. We see an awful lot of tactical deployment of technology, which means it is a case of saying, 'That's your problem, not mine.' The responsibility is pushed down the food chain in an organisation, rather than being recognised as something that is very valuable.

Ms PLIBERSEK—Do you mean that a CEO does not need to know how to hack into someone's computer but they need to know that it can be done to their organisation, and they don't know?

Mr Ferguson—Correct, and they need to build some management policies and deploy a culture of security that encourages everyone to follow those practices that get put in place.

Mr Hurt—One interesting challenge that a lot of organisations have is actually putting a true value on their information assets. So where organisations are often very well informed on how much it is actually worth to them to have physical security—things stolen et cetera—they actually do not have a true value of the information asset in their databases; for instance, how much their customer database is worth to the corporation.

Ms PLIBERSEK—And how much would it cost to fix the problem if they—

Mr Hurt—Yes. We submitted in the paper a number of tables, for example, to put a rough scale against certain assets, to say how much it would cost if it was lost or damaged, whether it is replaceable and those kinds of things. I think that is a very important aspect in valuing a corporate asset in an information sense.

CHAIRMAN—You say that senior management must be involved in the risk management strategy. Back in the early days of IT wasn't it true that a lot of technical people in the industry—with the greatest respect to our systems engineer here—drove the whole thing and companies wound up with reams and reams of information that management could not digest; they did not understand what the hell it meant and did not need and did not want to. It was an axiom at that time that management needed to be involved in the design, at least in the overall specification of what they wanted the system to accomplish, before you went from paper to the computer based system. Is that true?

Mr Ferguson—Absolutely.

CHAIRMAN—So nothing has changed?

Mr Ferguson—Nothing has changed, and we have seen a very recent iteration of that with the prolific acquisition of IT in the late 1990s, when everybody got on the Internet bandwagon and everybody had to have a web site.

CHAIRMAN—I am willing to bet you that a lot of people wasted a lot of money.

Mr Ferguson—I would agree absolutely. What we are talking about is very plainly the acquisition of technology without some business driver. We saw a lot of that—'My competitor's got this so I have to have it'—without necessarily saying this is the business need and this is what we are going to require to meet that business need. The implementation of security is exactly the same. It really needs to start with a business requirement and an assessment of the risk to the assets as well as an assessment of the value of the assets and then some management goals and objectives around the whole deployment. Then you can start to look at: so what technology fits us?

Mr Hurt—We are also seeing a lot of organisations actually taking the primary responsibility of security. A chief security officer originally resided in IT underneath the chief information officer, instead of reporting to the board itself. The post is now seen as an important key role in the organisation that crosses all of the bounds of the organisation, not just IT.

Senator LUNDY—That is a very interesting point; I would like to develop it a little further. I notice that in your submission you have raised the spectre of internal auditing as a way of introducing accountability and potential enforcement, particularly as it relates to your emphasis on management processes. Is an internal or external audit of your security measures the only way to introduce accountability into either public or private corporations over this stuff? If it is not, what other avenues are there for an external assessment of performance of security risk management within a given organisation?

Mr Ferguson—There are a number of functions that are covered by the term 'audit'. There is one function that is very much about accountability and there are—

Senator LUNDY—I am thinking more of it in the context of performance.

Mr Ferguson—There are many software tools available that enable an ongoing audit process that examines the security policies and the rules basis and things that are in place and ensures consistency and also ensures the ability to update and change in a very efficient manner. Auditing is not a one-off process; it is ongoing and continual.

Senator LUNDY—Do you see performance auditing as a key tool for management trying to educate themselves about these issues?

Mr Ferguson—Absolutely, because auditing—and auditing tools—is the bridge between all these technology things and what is really happening within the business.

CHAIRMAN—Then you would agree with us that the private sector need to incorporate in their annual reports performance auditing as well as strict accounting auditing?

Mr Ferguson—It depends upon whom you consider to be the audience for the annual report. If it is the shareholders, absolutely.

CHAIRMAN—Yes, it is your shareholders. Thank you, that was very good.

Senator LUNDY—As a company working in this space, how do you help demonstrate to your clients what you have been able to achieve with other clients? What do you use as your reference base?

Ms PLIBERSEK—'We would like to be able to tell you but we would have to kill you.'

Senator LUNDY—I am not asking the question very well. It really goes to what external measurements are available as to your performance and if there is an enforcement mechanism associated with the standards that apply in this country. If so, what is it or is it really such a new area that there is no enforceable regulatory base against which you have to formally measure up?

Mr Ferguson—Can I give part of an answer to that? That is a question that we might take on notice and answer in a slightly different way.

Senator LUNDY—Sure.

Mr Ferguson—Primarily we use organisations that have successfully deployed a security environment in line with either the international or Australian standards. We think the standards, when it comes to giving a framework on which to craft a policy and then deploy some technology, are actually quite good. In fact, although there are only 13 people in the organisation here, we have a security policy that is in a document of about 680 pages that covers not just information technology but security of people, premises, equipment and all sorts of things.

CHAIRMAN—Six hundred and eighty pages! Has anybody ever read it?

Mr Ferguson—Absolutely. I have read it three or four times and we continually update it.

CHAIRMAN—Do you know the finish yet?

Mr Ferguson—No. There is no finish.

Ms PLIBERSEK—He keeps falling asleep before the end!

Mr Ferguson—The good news is that it is very well referenced and cross-referenced.

Ms PLIBERSEK—It has big writing: it has 680 pages but it is only 2,000 words.

Mr Ferguson—Perhaps it is a little over the top, but we deliberately undertook that process to have a model and a basis on which to principally work with our business partners and our channels to help them articulate the need back into the end-user community. As a business, we do not transact business directly; we only go to market. We support and sell our product through third-party organisations. There is a lot of individual expertise and there are a lot of services associated with deploying a security environment. Ours is only the technology element.

Senator LUNDY—We heard from Standards Australia earlier today about the standards that are in place. Presuming that all the work you do complies with Australian standards, who checks that? What is the quality assurance mechanism in Australia that enables people procuring your services to contest or know that you are complying with these standards?

Mr Ferguson—I would say that the primary quality assurance is the penetration testing that is done.

Senator LUNDY—So it is an outcome test as opposed to a prescriptive input test?

Mr Ferguson—Yes. You can measure the quality as much as you want but it is result that is relevant or pertinent to business.

Senator LUNDY—So some sort of performance audit would be the only mechanism to delve into whether or not each prescriptive element of Australian standard HB231: 2000 is complied with.

Mr Ferguson—That is why we ended up with 600 and something pages.

Senator LUNDY—I think this is a really important point to get our heads around: the relationship between the standards and the proof of them working is outcome driven, and the performance of the solutions themselves.

Mr Ferguson—That is the same in any business. We view government as a business these days because that is very much the way it is structured—properly and correctly. The reality is that you can be as secure as you want if you have an unlimited budget. There will always be compromises in the implementation. Again, that is why it is critical that the appropriate risk assessment and the evaluation of assets are done upfront because then, as an organisation and as a manager, you know where to deploy resources in some kind of prioritised way.

Senator LUNDY—As a company selling through a third party, how do you get that message through about issues like industrial democracy and engaging with employees through appropriately structured forums in the workplace? It is a key part of the jigsaw puzzle that makes up your solution, but how do you get that through the vendors that you work through or the companies that you sell through?

Mr Ferguson—Firstly, the companies that we work through are companies and organisations that are in the business of security and that understand the issues. We are quite selective about the organisations that we choose as what we call business partners, as opposed to just somebody who resells a product. We test and audit their capability and competency. We look at three particular aspects for an organisation. We look at the people, the processes and the infrastructure that they have in place to ensure that they can deliver in line with what we feel the market needs. That is something that is audited on an annual basis.

Senator LUNDY—My final question relates to your earlier comments regarding Gatekeeper. Do you, as a company providing a PKI solution, feel that you are competing with that government solution? Is that how that works? I am not sure how you see Gatekeeper operating in the market. Obviously you have a different solution, but do you perceive that the government is competing in a place in the market where the private sector is providing commercial solutions?

Mr Ferguson—Firstly, we have a view that anything that is open source or anything that is readily available is almost by definition insecure. The more available something is the more available it is for anyone who wants to really have a look at it and find out the ways of circumnavigating or cutting through a piece of code. Secondly, we have a very strong view that there is no one organisation or company that addresses all facets of security. Both technology and the market are still relatively immature and what we are seeing is an emergence of best of breed organisations in very specific aspects of security. Thirdly, we have a very strong belief that, given the dynamic nature of the issues around security in the market, the solutions that are implemented must be software oriented, because it is only a piece of software that you can continually and dynamically update, modify and integrate with a third party.

Senator LUNDY—That does not answer my question.

Mr Ferguson—It does not answer your question. From a government perspective we have to be seen to be competing with Gatekeeper because it is there as a function. It would not be

necessarily our recommended method for securing an environment, but it could be one part of the puzzle.

Senator LUNDY—Does Check Point operate in overseas markets?

Mr Ferguson—Yes, everywhere around the world.

Senator LUNDY—Do you know of other jurisdictions that have a publicly driven PKI system like Gatekeeper or equivalent?

Mr Ferguson—Yes. The US government has—

Senator LUNDY—You can take that on notice.

Mr Ferguson—Yes, I will take that on notice and come back and answer that a bit more fully.

Senator LUNDY—It would be interesting to know, if you have that information. I am not trying to give you work. We could do the research ourselves, but if you have an insight that would be helpful. Thank you.

Mr Ferguson—There is just one last thing. The issue of security is about a lot more than authentication. That is why I am saying there are multiple elements to building a holistic security solution. So Gatekeeper is both competitive and potentially complementary.

CHAIRMAN—Can I point out to you something we heard earlier today. Your statement was that open source was more subject to security breaches than closed source. We heard the opposite view to that—that open source was better because it was open, people found out there was a problem quickly and they had no reason to hide the errors. There was no justification for hiding in there, whereas with closed source you do. I just put it to you as one of the things we heard.

Mr Ferguson—How long have we got?

CHAIRMAN—We don't have long; we have to move on to our next witness. We really thank you for appearing today. If we have any further questions, you won't mind if we put them in writing to you?

Mr Ferguson—Not at all. We do have a couple of points here that we will come back to you on.

CHAIRMAN—As with every witness, we will send you a copy of our report.

Mr Ferguson—Please do. Thank you.

[2.45 p.m.]

KIDD, Mr David, Solutions Architect, SingTel Optus Pty Ltd

McCULLOCH, Mr David, General Manager, Government Affairs, SingTel Optus Pty Ltd

REICH, Ms Jill, Sales Executive, SingTel Optus Pty Ltd

CHAIRMAN—I welcome the witnesses. We have received your submission. Do you have an extremely brief opening statement that you would like to make, or shall we start asking you our penetrating questions?

Mr McCulloch—We have about three minutes of opening statement.

CHAIRMAN—Can you make it shorter, please?

Mr McCulloch—Yes, I will. Before I do that, could I make one correction to our submission?

CHAIRMAN—Of course.

Mr McCulloch—The first line of paragraph 4.28 currently says:

The PSM guidelines classify information using the following criteria ...

That should read, 'the problem is that the PSM guidelines should, but do not classify information using the following criteria …'

I will be very brief. Optus has considerable experience in providing products and services that process, store and transmit electronic information on behalf of the Commonwealth, and that experience allows us to make some observations in relation to the Commonwealth's current security guidance framework. Jill and David deal with those issues on a day-to-day basis with government clients and our vendors, and they are experts in this field.

Our submission highlights three main areas where current arrangements impose unnecessarily high costs for the Commonwealth and business. The first issue is the process that enables products to be listed on the Defence Signals Directorate's endorsed product list, the EPL. We do not list products on the EPL but our partners and suppliers do. The process for listing is costly and time consuming and it acts as a deterrent to list new products. The reluctance of vendors to list products restricts our product choice when developing bids, and the Commonwealth faces risk as a result of the slow pace of the approval process. Commonwealth staff are forced to use outdated products with limited support from manufacturers, and the Commonwealth is then open to risks associated with product faults not being repaired. The EPL process is mandatory in application and there is no flexibility for minor modifications and the like. We think that the process should be streamlined and made more flexible. Our recommendation for faster approval

of products, both software and hardware, that have already gained an EPL listing but have been modified or upgraded would be of immediate benefit to business.

The second area relates to inconsistent security standards operating between Commonwealth agencies, between governments and between all levels of government and business. The current system of inconsistent standards, particularly between Commonwealth agencies, is inadequate and costly and our submission makes some specific recommendations about the development of a graded standard that could be applied to all organisations that handle Commonwealth derived and personal information. In other words, in the Commonwealth framework there needs to be specific recognition given to systems that meet other standards.

The final area is security classification methodology. What tends to happen is that a classification is given which relates to the most valuable information. That then requires a gold-plated solution. Agencies, we think, would get better results and more economic solutions if they imposed multiple security classifications. That means that, when guidelines are being applied, there needs to be greater consideration of the value of the information being protected, the efforts that an attacker must undertake to compromise the information and the additional costs associated with encrypting overclassified information.

The other problem in terms of the guidelines is that, once protected classification is required, there is no flexibility in terms of the secure facility that must be provided. As our submission points out, in the case of Optus there is no recognition, for example, of the security features of our private secure Internet; it is simply treated as the public Internet. That means that an expensive solution—and an unnecessary one, we would submit—needs to be implemented. Our submission goes into a bit of detail about an arrangement we have had with the Health Insurance Commission. In that instance, the HIC was not able to use our carrier grade security controls and procedures as the Commonwealth does not view them as appropriate. We had to include an accredited T4 secure facility and, in our view, that added unnecessary costs. That completes a brief summation of the issues raised in our submission and we would be happy to answer questions.

CHAIRMAN—Thank you for that. Does Optus believe that open source is more secure or less secure than closed source?

Mr McCulloch—That is certainly not an issue within my expertise.

Mr Kidd—We are not really a vendor in terms of that sort of technology, so it would be hard to make a call on that as there are conflicting issues.

CHAIRMAN—But you have to deal with it.

Mr Kidd—Not in terms of the systems. If you look at the systems that Optus uses to implement communications services, they are basically in the former area, the proprietary type technologies. Router operating systems and carrier switched operating systems tend to be proprietary operating systems and they tend not to be open source. We might use open source as part of the management of those systems in terms of desktops or network management platforms that provide views for those carriage networks. However, the technology in the carriage networks tends to be very proprietary.

CHAIRMAN—You talked about deficiencies in IT security, particularly in terms of differences between jurisdictions, namely the Commonwealth versus Victoria, New South Wales, the ACT government or whatever. However, I note that to the best of my knowledge you have not applied for Gatekeeper accreditation. I wondered why that was.

Ms Reich—Because of the expense and because the perceived benefit is not yet visible to us.

Ms PLIBERSEK—How much would it cost you? Have you done a business case?

Ms Reich—No, we haven't directly, but we work with a partner—VeriSign—which has been through Gatekeeper accreditation and is the only company that can issue Gatekeeper certificates with the full ABN-DSCs. They were talking about millions of dollars worth of investment.

Ms PLIBERSEK—But you probably do not need to do it if you work with them regularly as a partner.

Ms Reich—That is right. They certainly have not received any return on that.

CHAIRMAN—My advice is that PricewaterhouseCoopers in beTRUSTed is also accredited to issue ABN-DSCs. Your submission refers to the development of a more efficient and cost-effective system to determine suitable products for DSDs in closed product lists. Do you work with DSD?

Ms Reich—We do not directly have any products on the EPL, but again, through one of our partners—ActivCard, which is now VeriSign—we have jointly developed a managed service called OPI Trust. That service is going through accreditation on the EPL and, to date, Optus has supported VeriSign to go through that process to the tune of about half a million dollars. We have been going through that process now for about 18 months.

CHAIRMAN—Are you saying that DSD is too slow and too expensive?

Ms Reich—I think the process is too slow and too expensive.

Mr Kidd—There is a secondary area as well that affects us, which is providing solutions to government customers. Many of those customers now insist that, if there is a secure solution end to end, it has to be with products that are on the EPL. When you are working in routed IP type networks there is a limited set of products actually on the EPL. Those products are very specific to the hardware and software versions so that, as soon as any changes occur to that hardware or software, which typically happens very often in that vendor environment, you are either living with an older technology that does not have the bug fixes in it or you are forcing that manufacturer to go through the same process again of spending in the order of half a million dollars to $1 million, plus six to 12 months going through the approval process.

CHAIRMAN—We have been told by a one respondent that we should be much more concerned about the system itself than we should be about the hardware.

Ms Reich—That is right—how it is actually implemented within the agency rather than the crypto technology or the hardware device.

CHAIRMAN—Would it not be ridiculous for the Commonwealth, which is an agency that really only transacts business within itself, to have the same security format as one that transacts business over the Internet with all kinds of clients and suppliers?

Ms Reich—I would have thought so. Absolutely.

CHAIRMAN—You are not saying that you want a uniform approach?

Mr Kidd—No.

Ms Reich—We want a more flexible approach.

Mr Kidd—We are saying that we want a layered approach which builds on standards that are in the marketplace—

CHAIRMAN—How can you do that when the Commonwealth is different from Victoria and New South Wales and you want them all to be the same?

Mr Kidd—That is a good point. I think they all need to be the same in terms of a base point. They may have variations to their requirements to match business requirements but they still should be based on a framework of standards that comes from a common base point. Then you increment standards based on a certain commercial level and a certain level for the next level of security, and it builds on top of that.

CHAIRMAN—Are you familiar with a document put out late last year by the Management Advisory Committee of the Australian Public Service called *Australian government use of information and communications technology: a new governance and investment framework*?

Mr Kidd—I have not read that one, no.

Ms Reich—No.

CHAIRMAN—Would you like to borrow this and write down how you get it and give it back to me before you go? Would you mind having a look at that and telling me whether you think that represents a good overall starting point for a strategy for the Commonwealth?

Senator LUNDY—You made a point in your presentation about having a particular solution but that that does not conform with the requirements of DSD. Can you step me through that again, slowly, particularly if you feel that it affects your ability to compete in that area?

Mr Kidd—The point behind that was the base level solution. Regarding Optus's base product sets in this IP space, David talked about how we have a service called Optus Private IP, which is essentially—

Senator LUNDY—Is it a virtual private network?

Mr Kidd—It is VPN over carriage infrastructure, so each customer looks as though they have their own unique private network and only those customers' end points can be members of

that network. That solution provides an end to end virtually private network for that customer, as if you were providing your own dedicated network for that customer. In the classification process that occurs that is just treated as another Internet solution. There is no delineation between that and any other Internet based solution.

Senator LUNDY—Under whose definition?

Mr Kidd—Departments consider carriage networks to be untrusted or insecure.

Senator LUNDY—It is a definition of a carriage network as opposed to a definition coming from the other end of a VPN. FedLink is a VPN, so it is good enough for federal departments to subscribe to the federal government's own initiative. I think—excuse the pun—that there is a complete 'disconnect' between their policy and what you are experiencing.

Mr Kidd—There is a policy. What FedLink says is that you do not trust any network, therefore you put an end to end encryption process in between the end points. FedLink allows you to operate over the Internet or any network and it provides an IPSec encryption capability at the end.

Senator LUNDY—You provide the same thing but essentially—

Mr Kidd—Yes, but it is over a private network. We are saying that once you have a private network with its own measures of controls and the difficulty of getting into and decoding the information, is it necessary to have the same level of encryption or security regime around that. FedLink was designed on the lowest common denominator basis.

Senator LUNDY—We heard that yesterday. What is the fix for your problem in that regard? What standard or guideline do you think restricts that?

Mr Kidd—One of the things we alluded to in there is that maybe what is required is an examination in the PSM of putting some more delineation or gradation in there about guidelines or recommendations into examining the type of network solution that is being used. At the moment, it is treated fairly black and white.

Senator LUNDY—Is that a subsequent standard that is evoked under the PSM, or is it an aspect of the PSM itself?

Mr Kidd—What tends to happen is that each government agency has their own security manual, if you like, or rule book, which looks at their business processes and interprets the PSM and ASC33 and says, 'Here is our set of guidelines.' Those guidelines are based around their business requirements.

Senator LUNDY—Have you encountered this problem just with Health or with a number of them?

Mr Kidd—A number of customers.

Mr McCulloch—Another issue is that once the information is protected to a certain standard, then ASIO accreditation requirements kick in.

Senator LUNDY—ASIO or DSD?

Ms Reich—ASIO for a security facility, a T4 accredited facility.

Senator LUNDY—Have you raised this issue specifically with ASIO or DSD?

Ms Reich—No.

Senator LUNDY—Certainly from DSD, we are getting a strong message that they would like to work closely with agencies and departments and people working in their space. In terms of providing security solutions to government, what is your structure? Do you work with vendor partners? Do you tender as part of a group? How is your relationship with the Commonwealth established?

Ms Reich—For example, in HIC and cluster 3, which are two examples where we provide protected level networks, we are the prime contractor to the government and then we subcontract the security aspects to other vendors who provide that specialist service.

Mr Kidd—They are driven by an RFP process so, typically, it is driven by a requirement. That requirement is interpreted, we then arrive at a solution and we look at which partners will be used to deliver that solution.

Senator LUNDY—Does that apply to their voice needs as well as data needs?

Mr Kidd—From a security point of view?

Senator LUNDY—Yes.

Mr Kidd—It has not been typical to date.

Senator LUNDY—So, it is just data?

Mr Kidd—Yes.

Senator LUNDY—Right.

Mr Kidd—Though it is becoming problematic now that voice over IP is starting to occur.

Senator LUNDY—How is that convergence impacting on that sort of separation of treatment of data and voice?

Mr Kidd—It does cause some problems. Our technical solutions and others have the ability to classify the data itself from a transport point of view, so we can transport data differently in the network. You can classify it for a number of different reasons. One of them could be that it is the type of traffic, whether it is voice, data or video. With that classification information, you

can then decide whether to encrypt it or not to encrypt it. Once again, as soon as you start doing that, you are then imposing more processing load on the equipment that is doing the routing. You will then slow down the router or require bigger routers and the cost will go up.

Senator LUNDY—As a company in that regard, how do you involve yourself in that decision making on behalf of your client? What opportunity is there to work through those issues with them, not only at a policy level but also at the next step which is implementation of that policy?

Mr Kidd—It is usually difficult because in an RFP process you are bidding against a competitor, therefore, you have to be careful that you are not providing a non-compliant solution. If it is part of what has been stated as a requirement in that RFP, then we have to be careful that we offer a solution that matches that requirement. With those sorts of mandates that say that the equipment has to be on the EPL list to provide this level of encryption, we have to respond that way otherwise we may be non-compliant. Then there is an opportunity to discuss with the department during the negotiation phase prior to implementation whether there are alternatives, and then it is really a case of how to implement that to meet that requirement. You have fewer options once you are at that point.

Senator LUNDY—In terms of generalities, how prescriptive are these contracts in requiring you to provide certain types of secure networks? Are they really prescriptive?

Mr Kidd—Some are and some are not; it varies. Some say that they have to have a capability. For example, they use words like IPSec, so they are getting reasonably prescriptive because of the technology focus. Some then go to the next point and say that they must be on the EPL and must comply with this and that, and even apply a set of processes and procedures that have to go around that. It does vary, but usually they are reasonably prescriptive.

Senator LUNDY—Are you able to make some observations about the attention paid to security related issues and how that has changed, say, in the last decade?

Mr Kidd—I have had limited experience in that area.

Ms Reich—It varies. It is very inconsistent and it is inconsistent within departments. Some areas of a department that have responsibility for security would be very cognisant of the risks and issues, and other areas pay less attention to them. Also, one of the antagonistic things that you see are practices going on in a department which are very loose in their security application, yet we are being asked to comply with a very tight set of standards, rules and procedures.

Senator LUNDY—We heard exactly this point from the previous witness: you can have all the technology specifications but unless you have management commitment and a culture of security—

Mr Kidd—Security is only as good as your weakest link.

Senator LUNDY—That is right.

CHAIRMAN—You have the wrong culture.

Senator LUNDY—Yes, if you have the wrong culture you can do all those things but there can be gaps because the management commitment is not there. That is obviously an observation that you would share.

Ms Reich—Yes.

Senator LUNDY—I am looking for your insight into how that can best be remedied. What do you see as your involvement as a service provider in making that work? It is tapping into your corporate knowledge about what is a good system of consultation and the creation of those security-positive cultures in an organisation. You do not have to reflect on anybody, but can you speak from your general experience?

Ms Reich—One observation is that there is not a good judgment of risk. People in security areas have the ability to see a set of rules and to apply them, but the ability to assess risk and to judge what constitutes a real risk and what is or is not pragmatic is an issue. The security culture is important but it is more a risk management culture as well. We deal with banks and other organisations that have an interest in securing information, and we deal with organisations that, for competitive reasons, need to secure information. Being able to draw on those experiences and feed them back into the Commonwealth and have them receptive to those ideas and concepts would be useful.

Senator LUNDY—You are about infrastructure. Are you aware of the federal government's plans—I think they are meeting today in Melbourne—to create a trusted information sharing network on critical infrastructure? Has Optus been involved in that?

Mr McCulloch—Yes, I am aware of that. I believe that Optus has had some involvement in that but I can certainly find out and get back to you.

Senator LUNDY—I would be interested in that. The protection of critical infrastructure is obviously a key aspect of security. As Optus is an infrastructure provider or carrier, I would be interested in your perspective.

Mr McCulloch—I think that is being organised through the Attorney-General's Department.

Senator LUNDY—That is right, yes.

Mr McCulloch—I am pretty sure that we are involved in that process.

Senator LUNDY—I do not know whether you have any observations that you want to share with the committee about that but it is very clearly driven by what I call a very light-touch approach in that they are hoping that information sharing amongst companies, agencies and so on will lead to something. I am waiting with interest, personally, but it would be great to get feedback from Optus about that as part of the big picture on security.

In relation to the issue of endorsed products—and I hear about this all the time—various companies usually have some issues about it. It is too prescriptive or irrelevant or out of date, or something like that. As a player in the various sectors, what role if any do you have in advising the government on what their endorsed supplier list should contain or how they suitably

represent eligible commercial providers or service providers? Do you have a role in that or do you just have to fill out a form to be an endorsed supplier? What is the process?

Ms Reich—Are you talking about the endorsed supplier process, not the EPL?

Senator LUNDY—What is the difference?

Ms Reich—The endorsed supplier process is about going through a whole lot of financial checks to be a viable supplier to the Commonwealth.

Senator LUNDY—And that is through the department of finance?

Ms Reich—Yes. And the evaluated products list is the DSD—

Senator LUNDY—Is that the second one?

Ms Reich—Yes. It is managed by DSD. To get a product or service on that list requires a complete process and a lot of documentation. It is a process within itself.

Senator LUNDY—And that is where you have hit the barrier—with that definition?

Mr Kidd—We have hit it from a user of technology rather than a supplier of technology point of view. By having to use technology to implement solutions for government customers we can only use products that are on that list. Even the variations of those products are on that list. So if we get to the point where there are features that we need or the government is interested in having but they are in a later version that has not yet been through the next phase of that process then either we are restricted in offering them or we have to qualify them and see whether the government then wants to take a risk and use a risk assessment. But, typically, that is not expressed.

Ms Reich—Or we might incorporate a product in a service or a solution on the EPL, and then suddenly it is taken off the EPL. So we are left high and dry.

Senator LUNDY—What do you know about the decision making process of the EPL within DSD? Do you know anything?

Mr Kidd—Not a lot.

Senator LUNDY—It is something that we can pursue with them. Is there not a lot of consultation with you?

CHAIRMAN—You do not know whether it is resources or culture or dragging their feet—trying to make life hard for you.

Ms Reich—I do not think it is DSD or the people within DSD. It is that the system that has evolved has become cumbersome and probably needs to be reviewed.

CHAIRMAN—We will take that on board.

Senator LUNDY—We can follow that up.

Ms Reich—For example, there are only three companies that are currently accredited to perform evaluations: TENEX, CMG Logica and CSC. So they can virtually charge monopoly prices to do that accreditation and they have a vested interest in dragging out the process for as long as possible.

Senator LUNDY—They are not Australian companies, are they?

Ms Reich—No. They are also competitors. We have a situation where we are directly competing against one of them for business and they have all our intellectual property of the solution.

Senator LUNDY—Was this as part of the assessment process? And you are competing against them? That is very interesting.

Ms Reich—That presents an issue for us. They assure us that there is segregation.

Mr Kidd—Chinese walls.

Senator LUNDY—I have heard that phrase too much in the last 12 months. But that is a very useful insight.

Ms Reich—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.

Senator LUNDY—Who does that accreditation?

Ms Reich—It is a combination of DSD, from their gateway certification process, and ASIO, who accredit the physical facility.

Senator LUNDY—I am finally starting to understand.

Ms Reich—Optus looked at becoming a provider of that, so it was a matter of augmenting our Internet services and our network by providing a secure gateway. We costed that at $1 million to obtain that certification.

Senator LUNDY—Do they charge for that accreditation—those companies?

Ms Reich—Yes.

Mr KING—With respect to the EPL, you would not argue about the competency or proficiency of DSD, would you?

Ms Reich—No, that is not the issue.

Mr KING—With respect to the fact that it is cumbersome, I would rather be satisfied that whoever is seeking to contract services from the Commonwealth is a secure and properly based organisation than be too worried about the fact that it might take a bit longer than you might like. What would you say about that?

Mr Kidd—'Cumbersome' is an interesting word because there are a lot of—

Mr KING—It was your word.

Mr Kidd—things behind that. There is probably a resourcing issue on both sides. There is also the fact that there are only a certain number of parties that are able to perform the accreditation process.

Mr KING—I gather from what you have just been saying that it is actually not DSD itself which evaluates the product lines; this is done by subcontractors. Your complaint is that they have an apparent conflict of interest.

Ms Reich—There may be. Also, DSD have had a lot of issues in actually retaining staff in the information—

Mr KING—Presumably they get poached by you and others.

Ms Reich—Not by us but by our competitors.

Mr KING—At the end of the day, if there is a subcontractor from DSD doing the vetting, am I correct in thinking that a DSD employee or staff member—a manager or officer at a sufficiently senior level—looks at reports, recommendations, and says, 'Yes,' 'No,' or is indifferent, or says, 'Let's put it out to tender again.' It is not just left to the subcontractors to decide. They do not delegate the decision?

Ms Reich—No.

Mr KING—That is comforting to know. I guess the only concern I have with the whole process is not with the competency of DSD, which I think is outstanding, but that I am not entirely sure how the Defence Signals Directorate gets involved in these issues outside the Department of Defence. But it does, so there it is. I suppose somebody has to do it. The other issue I wanted to raise with you is this whole idea of a consistency of approach that you seem to be concerned about. In the modern world where you have different Commonwealth agencies acting independently of each other and independently of the Commonwealth, I am not quite sure I understand your point. I would have thought it was important that you have to deal individually with each of those potential purchasers of your products and not expect to have to deal with one on the basis of one suits all. What do you say about that?

Ms Reich—It is really a two-way street. If we could say to a state government agency, for example, 'This service product solution has been deemed suitable by a Commonwealth agency and their security requirements are X, Y and Z and they have a protected level network,' the state agency would be able to accept that and say—

Mr KING—I don't see that at all. I was head of a Commonwealth agency for 3½ years, and a United Nations agency as well. They had different standards because they had different security risks. I don't understand why you would want to impose the cost of a high security risk rating for the supply of information or information systems on one organisation and then impose the same cost structure on another. I would have thought that what is important is that that organisation profiles itself having regard to its own risk assessment, which is presumably a proper one—and there are people who check these things. Basically, it is a matter of needs versus the product that is being purchased. The fact that you might have to do 100 different assessments is just part of the ordinary workings of the marketplace.

Ms Reich—I think we are saying the same thing. We are agreeing with you that it is a cost burden for agencies to have to pay for overclassification. If there were a common set of standards so that people understood how they could actually measure the value of their information then we would all be talking a common language and have a common understanding. We would have a common idea of the security level that needed to be provided.

Mr Kidd—We are not necessarily saying there is just one standard; it is a layered approach to standards.

Mr KING—So you are not arguing that you really only want to deal with one person?

Ms Reich—No.

Mr McCulloch—The key issue is that the agency has an open mind and is not simply being dictated to by the standard of its own government; it will consider afresh the fact that it has been classified elsewhere.

Mr KING—Or the department secretary, if it is an agency of that department. That is usually the problem, in my experience. I have one final question about NOIE. What interaction do you have with NOIE?

Ms Reich—It is very limited, from my point of view. David, you have more interaction with them.

Mr McCulloch—From a policy perspective we deal with NOIE on a number of issues from time to time. We have a very wide ambit in terms of the information economy.

Mr KING—Are you impressed with the quality of their work?

Mr McCulloch—I think NOIE does a good job in advancing the information economy policy issues together with DCITA.

Mr KING—Would you tell us if you were not impressed?

Ms Reich—I think they have less influence.

Mr KING—I just want to know.

Mr Kidd—Maybe not.

Mr KING—Thanks very much. That is very helpful.

CHAIRMAN—Thank you very much. We have to get along. If we have any further questions, you would not mind if we put them in writing, would you?

Mr Kidd—No.

CHAIRMAN—We will send you a copy of our report. We thank you very much for your submission, your attendance and your open answers to our questions.

[3.23 p.m.]

CROMPTON, Mr Malcolm, Federal Privacy Commissioner, Office of the Federal Privacy Commissioner

PILGRIM, Mr Timothy, Deputy Federal Privacy Commissioner, Office of the Federal Privacy Commissioner

CHAIRMAN—Welcome. Thank you very much for your submission and for coming today. I will now publicly apologise for the absence of my colleagues. We will proceed, and I will turn into a pumpkin in half an hour or two because I leave for another aircraft. Computer Associates Australia, in appearing before us today, said something to the effect that we—Australia—do not assure privacy to the extent that it is assured in Europe. Then they said we do not yet enforce privacy. Do you have any comments about those statements?

Mr Crompton—It would be a very sweeping statement that would need some unpacking, including as to whether they were talking about public sector privacy or private sector privacy, and even within those sectors it would need further questions to unpack the question. However, I will give you an answer that will show you the complexity of answering the question. A couple of years ago a group called Consumers International—and we can give you the URL link to their report—did a survey on the extent to which there was privacy online in the private sector. To their surprise they found that, while there were stronger laws in Europe for protecting privacy, at the margin there was better privacy protection in the USA. The state of the law is only one of the measures you need to look at before you reach conclusions.

CHAIRMAN—Thank you. For the public record for whatever it is worth, in 1997 we held an inquiry into Internet commerce and the use of the Internet for online purchasing. The most headline grabbing of our recommendations was that we have federal legislation with regard to private sector privacy requirements. That, of course, was against government policy and the Prime Minister's statements and everything else, and we won. I know you were not the Privacy Commissioner then, but the then Privacy Commissioner appeared before us and made a strong case, as did the banks. They also said that Europe was very rule bound, but not necessarily outcome oriented.

Mr Crompton—The Consumers International report would still raise the same question mark. Efficacy still has to be one of the key criteria of any regulator. You only need just enough law that is necessary to get the job done and you have to see that the law you have and the other techniques available to you are effective. The review announced by the Attorney-General of private sector privacy provisions to take place at the end of this year will be about exactly that question. It will be about how we have affected the private lives of Australians. What impact have we had on the ability of business to do business? While it is a private sector review, you can possibly have strong law and poor enforcement, and the US has clearly set out to use existing law and to make it very effective. You can encourage the marketplace to provide solutions. It is a very complex mix. I do not think that you can deliver without the law and you cannot deliver by ignoring the markets. You also have to be aware of the technologies that are coming along and stay on top of them all.

CHAIRMAN—We have already mentioned the public and private privacy sectors, and you have responsibilities in respect of each of those. Are many privacy breaches in the public sector reported to you?

Mr Crompton—We have given you a little graph in our submission. It is on page 11 and it covers that point.

CHAIRMAN—With the greatest of respect, I do not think I am going to get much value out of that. Can *Hansard* record that it is one big black blob?

Mr Crompton—Let me show you our version. What is very interesting about the shape of that graph is that those are the complaints under the information privacy principles relating to Commonwealth public sector agencies. It leaves out the ACT, the part IIIA of the act which relates to the credit reporting industry and the private sector. You can see that, after some peaking two or three years after start-up, where the highest level of complaints was it has tailed off for a number of years. However, I would argue that, for a number of reasons, the level of complaints has gone up. That would have to include the fact that we have introduced private sector privacy law which, of itself, will have re-engaged interest in issues with regard to the public sector. We have set out to be educative in the way we have done the work and to bring the issues to the attention of the public where we can through the media and so forth.

I think there is also very little doubt that new online activity has generated interest anyway. You could argue that for many years the historical interest was Big Brother—big government. To a degree it moved on to Big Brother—big business—and the Internet has really made it distributed Big Brother or little brother or whatever you call it. It has reignited a lot of concerns in the data protection issue, and then it washes back into the more traditional areas of interest such as we are seeing there.

CHAIRMAN—There were 118 last year. Were many of those serious? Were many of them upheld?

Mr Crompton—The deputy commissioner is in a much better position to answer that than I am, and I will hand over to him.

Mr Pilgrim—In response to the question of whether many of them were serious, we will naturally treat the complaints of everyone who comes to the office as being serious because they will affect individuals in different ways and different capacities.

CHAIRMAN—If they are valid.

Mr Pilgrim—If in fact they are valid, that is correct. I would have to get back to the committee with an exact number of how many were upheld and what percentage of those could be —

Ms KING—What were they approximately—a half or a quarter?

Mr Pilgrim—I would be saying that over a half were found to have been upheld with regard to individual complaints. The severity of them can vary a bit depending on the outcome of the

remedy that the individual is looking for as well. In the majority of our cases it is important to note that we work on a basis of alternative dispute resolution procedures whereby we try to conciliate our outcomes. We have managed to conciliate in the life of the operation of the act in excess of 90 per cent of those cases without having to resort to using formal powers to issue determinations. Another important fact to give to the committee as well is that there are powers for the commissioner to encourage the payment of compensation and the like. What we have found is that in the majority of cases—in excess of 80 per cent—the majority of people are satisfied with an undertaking by the organisation that they will remedy their practices. The individual receives an apology from the organisation where there has been a breach, rather than immediately trying to get monetary compensation. That is a procedure we are also taking over to the private sector.

CHAIRMAN—Do a lot of them have to do with Centrelink?

Mr Pilgrim—Interestingly, I would say that the majority of our cases do not come from Centrelink, if you were to break up the figures—

CHAIRMAN—They would come from whom?

Mr Pilgrim—I would have to get back to the committee with a break-up, but there is a fairly equal distribution between the major organisations, such as the tax office, Centrelink and the other agencies that hold large amounts of the community's data. Centrelink themselves do handle quite a lot of complaints. As the committee may be aware, we have a process where we try to encourage the complainant to resolve the issue first with the respondent organisation before bringing it back to us.

CHAIRMAN—The reason I asked the question about severity is that we have a very real interest in fraud and the reporting of fraud, as you can imagine. I simply point out that we still call it fraud if someone in the tax office accesses somebody's tax file on their computer without having authority to work on that particular item, whether they downloaded it or used it or were just interested. That is called fraud. I have a different view of fraud, if you can understand that.

Mr Pilgrim—In those particular cases the individual who is affected—or the complainant—could bring a case against Centrelink with regard to an officer browsing when they should not have been going through someone's personal information. If that were to come before us, we would tend to want to ensure that the organisation—the tax office, for example—had already commenced their own internal disciplinary procedures in that case. We would want to see the outcome of that investigation prior to us pursuing the complaint because, if a suitable remedy is undertaken against the individual who undertook to browse or undertook the fraud, we would want to assess whether an adequate result had come out of that investigation before we would proceed.

CHAIRMAN—The point that I make is that, as with the issue of fraud, privacy falls in the same category in that there are true differences of severity. We can castigate ourselves, beat our ourselves around the shoulder with the proverbial whip and say how bad we are and then go to some of our South-East Asian neighbours' countries, see what fraud really is and then ask what privacy is and get a whole different generic definition. So sometimes we can get a bit carried away with ourselves.

Mr Crompton—There are two levels to think about. One of them is what you have been asking about, which is where design systems go wrong. It may be because there is a security breakdown or there is malevolent activity within the organisation. It would appear from the kind of complaints that we get—the level of them and the severity of them—that the Commonwealth is not doing a bad job in this area. You get volume problems, where a mass mail-out from something as big as Centrelink, but not just Centrelink, goes badly wrong. Then you can say, 'It's gone wrong for hundreds of thousands people.' It has probably not necessarily gone severely wrong for those people, but sometimes it has—like if you have literally published their tax file number, which is what can happen. These days Centrelink takes a much more aggressive approach to it than it did before. It will pulp a whole mail-out, if it has an inkling of it going wrong, rather than risk it. That is a good approach.

Mr KING—MPs have been known to do that, too—

Mr Crompton—Yes!

Mr KING—by accident, normally.

Mr Crompton—Of course. I would have to say that an issue that is probably just as important—and over time is probably a much more important issue in a country such as ours—and where there does appear to be integrity in systems, once established, is the design of the systems in the first place. Should we be allowing this data match to happen? It is not just a matter of checking if the data match happened as allowed by law, rather: should we have allowed it to happen in the first place? How do we respond to cyber crime? How do we respond to various national security threats? How do we respond to cradle to grave monitoring of a person who is oftentimes in the dole queue? Those are possibly the more privacy invasive questions, and they are sometimes being cooked very slowly so that, unless you stop and really contemplate, you do not actually notice it happening.

CHAIRMAN—I understand that. We have already talked to the department of health and we will talk to HIC. One of the big issues is that they would love to go electronic with people's individual health records rather than have the bits and pieces of paper at doctors' surgeries. There are some individuals, though, that scream about privacy. They are frightened to death that anybody would ever find out their health record, whereas I could give less of a stuff! It does not bother me one way or another. Some of it is individual choice isn't it, to an extent?

Mr Crompton—It depends on our life circumstances. Somebody such as me, who is fundamentally a healthy person feeling comfortable and competent in the society around them, really has a very different life experience from somebody who is marginalised in any number of ways. They may either have a very sensitive health complaint—say a mental health issue—or for other reasons their perspective on life could, perforce the circumstances of their life, be very different. I came across somebody a number of years ago who really made me stop and think. She was physically disabled and she was saying to me that as a good member of society she wanted to participate in society. She needed daily bathing, which had to be done for her. She was quite happy for that to be done but, when the carer turned up with six others, unannounced, to show them how to bathe her, she was mightily offended. She said, 'All they had to do was ask me first, and treat me with respect and as an individual, and I may well have said yes. But

just to assume that I was a dummy ready to be shown off was highly offensive.' We need to think about the great range of circumstances in our society—we really do.

CHAIRMAN—I have no trouble understanding that. Mr Crompton, you made seven recommendations. The first one was:

That those Commonwealth agencies with significant personal information handling responsibilities be required to report to the Privacy Commissioner, annually, regarding the number (and nature in trends of) privacy complaints that they handle.

That is a big ask, isn't it?

Mr Crompton—What is interesting is that we have done that by trying to get direct resolution between complainant and respondent, and all the time trying to achieve low-key, cool temperature results rather than taking angry adversarial approaches to resolving complaints. One of the artefacts of doing that is that you do not actually get a proper grip on how often the system is going wrong. So all we are asking for in recommendation 1 is that, in an objective accountability sense, we have a clearer view of the total range of complaints being received. I think it is highly admirable that Centrelink, for example and in particular, sets out to and strongly encourages people to get their complaints resolved early within Centrelink. I think that is excellent; that is the way it should be. But it does mean we may have an underestimate of quite how often things are going wrong or what the systemic issues are. I think, just in terms of pure accountability to the people of Australia, it would be worth while having a fuller picture.

CHAIRMAN—You are not asking for this to be public information, are you?

Mr Crompton—I do not see why not. If they already have the data, simply putting it into their annual report and saying that, while there were—I am picking a number out of the air—50 or 100 complaints dealt with by the Privacy Commissioner, we dealt with about 1,000 complaints in the Centrelink system. In a sense, that will be a measure of success, not of failure—that any human system can have glitches. That they are able to show there is a willing, fast, positive response when it does go wrong is probably an admirable result.

CHAIRMAN—Who is going to require them to report to you?

Mr Crompton—The obvious place to do that is in the annual reporting requirements.

CHAIRMAN—That is up to us.

Mr Pilgrim—To add to that, the majority of the agencies that we have listed, through their requirements under developing customer charters, would already be collecting statistics in relation to complaints to their organisations and would probably break them up into categories that would allow ease of producing that information.

CHAIRMAN—Recommendation No. 2 states:

That Commonwealth agencies be required to undertake privacy impact assessments at the beginning of the development of new proposals and initiatives involving the handling of the personal information of the Australian community.

Again, it is 'be required to'. How do we go about that?

Mr Crompton—As you have seen in our submission, a number of countries have begun requiring that of their government agencies. The most recent decision to do that was at the federal level in the United States. An act of congress was passed only two or three months ago. So that requirement is not uncommon. Just as we have environmental impact assessments being done, we suggest that the same thing be required here. It need be nothing other than an executive decision of government through the cabinet handbook rules or something like that, or you could move it up to a legislative model if that is what you want to do, but a privacy impact assessment helps you to get it right. It may be a financial saving device as well as a privacy improvement device, because there is nothing more expensive than retrofitting solutions down on an already designed system, whether it is bolting on security, bolting on privacy or bolting on anything else. It is best to put it in at the design level.

CHAIRMAN—Recommendation No. 4 states:

That the Committee endorse the approach announced by the newly established Information Management Strategy Committee ...

I do not know who that is. I have in front of me a document called *Australian government use of information and communications technology: a new governance and investment framework*, which was put out by the Management Advisory Committee and tabled last October.

Mr Crompton—I cannot read it upside down, but I am pretty sure it is the same thing. There is the statutory Management Advisory Committee under the Public Service Act. They commissioned, I think, John Rimmer, as the head of the National Office for the Information Economy, to produce the report. A number of recommended structures came through in John Rimmer's report. In a couple of our recommendations we have recommended good use of this framework being put up through that committee report.

CHAIRMAN—Could you come back to us and confirm that you are talking about this document?

Mr Crompton—I certainly can.

CHAIRMAN—I cannot tell you the committee's judgment but I know that two or three of us think it is not bad. I also noted recommendation No. 7 that your office be resourced to discharge the additional functions arising from the implementation of these recommendations. That was not a bit self-seeking, was it?

Mr Crompton—No, and I am perfectly willing to defend it. Before I answer the question, by the way, I do confirm that that is the document that I am talking about with regard to the previous question. With regard to resourcing, when you think that we are delivering a privacy regime for all federal agencies for the whole of the private sector as covered for something like $3½ million, we are an extremely lean organisation.

CHAIRMAN—Do you mean you are cost-effective?

Mr Crompton—I would like to think so, but that is also for others to judge. I also have to say that that leaves us with no fat left to do extras. We constantly come under pressure to do a little extra on the side in this area or that area and we are basically trying to say enough is enough. The Attorney-General holds exactly the same point of view. In August 1998, he wrote to all his colleagues telling them that from that point on, whenever they put up proposals that have a privacy impact, particularly on the operations of the Privacy Commissioner's office, the proposing agency or minister had to identify the costs for the Privacy Commissioner's office of doing that. That simply reinforces that far too many of the proposals that come forward do not recognise that there is a regulatory impact. You may recall a proposal put forward by Customs last year as part of the terrorism legislation in respect of which Customs was pulled up at the committee stage of the debate on the bills for not having consulted with the Privacy Commissioner's office on its proposal. When it did consult, it found that it was introducing new techniques that would require additional policy advice and additional auditing from us that needed to be funded. As a result of that a very small sum of money—we are only talking about something like $70,000 or $80,000—has been provided to our office to allow us to discharge the new functions that come to us because new law has been put into place. That is all we are saying. It is a basis for fully costing proposals; it is nothing more than that.

CHAIRMAN—We will take that into account.

Mr KING—I am interested to explore the boundary between expediency and privacy. It strikes me that if government is to work effectively, information from one area ought to be available to another in order to prevent fraud and to make decisions more expedient in so many different ways, including faster, better informed and so on. What do you say about where the boundary lies between the two principles?

Mr Crompton—That is an extremely good question. None of us likes to have to ring government up 20 times to say, 'Please change my address.' We would like to be able to ring up once. On the other hand, there will be people who do not want that to happen, who do not want their datasets to be connected. We have to work through the complexity of doing that. The UK Cabinet Office report which is mentioned on page 33 of our submission recognises exactly the conundrum you have identified. Essentially it is saying that government has an obligation—and it is an expectation of the citizenry—that it makes good use of the information in front of it, whether to improve transport planning by connecting datasets and understanding demographics, or in policing or health systems design, but it also has to gain the trust of the people in doing that.

As I have said before, and as I have said many times elsewhere, privacy is often nothing more than common courtesy: 'If only you had asked, I would have said yes.' This document from the UK recognises that empowering the citizenry to say yes or no will actually induce more yeses, not fewer yeses, because people understand that they can access their information, they know where it is going and that they will be pleased with the result. That is in contrast to what happened in Canada in 2000—and I have a press release about this—when they merged departments and went into the superdepartment mode that Australia had embraced a few years earlier. The superdepartment found that it had a lot of datasets so they said, 'Why don't we jam them all together?' They did that and they caused a furore and it took two weeks of hot parliamentary debate for the government of the time to decide to take that dataset to pieces because the people of Canada did not trust the government to have a cradle-to-grave dataset which is what they had created.

Mr KING—But should consent be the boundary?

Mr Crompton—It should be one of them.

Mr KING—What are the other considerations?

Mr Crompton—We need to remember that, in many circumstances, government is very special compared to the rest of the lives around it because it uniquely has the power to coerce.

Mr KING—But it is not profit making—

Mr Crompton—No, but you are compelled to be on the electoral roll. You are compelled to be taxed. Does that fact that you have been compelled to provide mean that there are special responsibilities on government to be open and accountable and not to go in for function creep? We are watching that all the time now. I think there are now 22 ways in which datasets from the electoral roll are fed out for what in many instances are admirable purposes—for example, health research, but many people thought they went on to the electoral roll in order to be able to vote, not to be part of a health survey and certainly not for direct marketing.

Mr KING—Is that happening?

Mr Crompton—Yes.

Mr KING—How are people getting access to the rolls for that purpose?

Mr Crompton—In the simplest terms, while electronic copies of the electoral roll are protected in law, these days we are seeing that technology has moved along and all you have to do is buy a physical copy of the electoral roll, send it offshore, get it scanned, bring it back, and each of those steps is a legal step. So we have in Australia—

Mr KING—Can you buy a copy of the roll?

CHAIRMAN—Absolutely.

Mr Crompton—As I understand it—and you had better check this with the electoral office if it is important to you—the electoral office has ceased to sell over the counter physical copies of the electoral roll. You can still go to the electoral office and inspect a physical copy of the electoral roll. They are investigating ways, check by check, of electronic access to the electoral roll. They have been quite thoughtful in how they are doing that, because as I understand it they have ceased to sell full copies of the electoral roll, the main reason being this fear.

Mr KING—It is a vexing issue. I agree that the British paper appears to set a reasonable balance between the two considerations. However, I would suggest that the mere fact that some people object to their information being disclosed is not necessarily a reason for not doing so, if other considerations of public convenience outweigh it.

Mr Crompton—Section 29 of the Privacy Act makes that an explicit obligation on us as we administer the act, whereby we have to take into account the balance between the public interest

in privacy and the public interest in government being able to govern, if you like, and business being able to do business.

Mr KING—Do you have a set of protocols that determine that issue?

Mr Crompton—I would point you to, in the law enforcement area, the very last page of our submission, where we set out a framework that we put forward for assessing law enforcement proposals that might be privacy intrusive. As you can see, it is a process of assessing the proposal and, if it gets through the assessment process, making sure that the powers are only used under the right circumstances; if they are used, that those powers are auditable; complaints against abuse of those powers can be heard; and that there is periodic review of the structure. So, yes, there are some frameworks. It is a proposed framework that we keep putting forward; we suggest that properly thought out law enforcement and national security proposals should pass a test like that.

Mr KING—I understand that you were recently appointed; is that correct?

Mr Crompton—I have been in the job for four years.

CHAIRMAN—You talked about some information from A-G's that you said supported your case. Is that letter from the Attorney-General public information?

Mr Crompton—I would have thought the Attorney should be asked whether that letter can be made available, rather than us. It is a letter he wrote.

CHAIRMAN—Mr Crompton, if we have further questions, you would not mind if we put them in writing?

Mr Crompton—Certainly.

CHAIRMAN—If, near the end of this inquiry, we decide to have a longer shot at these seven recommendations, you would not mind coming back to talk to us?

Mr Crompton—It would be a pleasure.

CHAIRMAN—Thank you very much.

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

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

Committee adjourned at 3.54 p.m.