COMMONWEALTH OF AUSTRALIA

Official Committee Hansard

JOINT COMMITTEE OF PUBLIC ACCOUNTS AND AUDIT

Reference: Management and integrity of electronic information in the Commonwealth

TUESDAY, 1 APRIL 2003

CANBERRA

BY AUTHORITY OF THE PARLIAMENT

INTERNET

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

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

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

JOINT COMMITTEE OF PUBLIC ACCOUNTS AND AUDIT

Tuesday, 1 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: Senators Humphries and Lundy and Mr Charles and Ms Plibersek

Terms of reference for the inquiry:

To inquire into and report on:

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

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

In conducting its inquiry the Committee will consider:

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

WITNESSES

Committee met at 9.36 a.m.

CHAIRMAN—The Joint Committee of Public Accounts and Audit will now continue taking evidence, as provided for in the Public Accounts and Audit Committee Act 1951, for its inquiry into the management and integrity of electronic information in the Commonwealth. I welcome everybody here this morning for the resumption of the committee's public hearings for this inquiry. Today we will continue to hear evidence from Commonwealth departments and we will also hear from representatives of one private company. Tomorrow the committee will move to Sydney for another public hearing, and further hearings will be held in Canberra, in May, during the budget session of parliament. I remind any members of the media here that reporting must reflect fairly and honestly the statements that are made today. Any violation of that will not be looked upon favourably by the parliament.

[9.37 a.m.]

BESGROVE, Mr Keith, Chief General Manager, Regulatory and Analysis Group, National Office for the Information Economy

DALE, Mr Tom, General Manager, Regulatory Branch, National Office for the Information Economy

GRANT, Mr John, Chief General Manager, Government Services and Information Environment Division, National Office for the Information Economy

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

Mr Grant—I have direct responsibility for the submission we have made.

Mr Besgrove—I have responsibility for issues to do with Gatekeeper accreditation, domain names authentication and e-security. I am also responsible for many of NOIE's research tasks.

Mr Dale—My responsibilities cover information security and a number of other online regulatory issues.

CHAIRMAN—Thank you, gentlemen. We also thank you for your submission. Would you like to make a brief opening statement?

Mr Grant—I do have a brief opening statement, but after talking to the secretary, I am prepared to forgo making that statement.

CHAIRMAN—Would you like to have your opening statement incorporated in *Hansard*? There being no objection, it is so ordered.

The statement read as follows—

Thank you for this opportunity to appear before you this morning.

I am John Grant - Chief General Manager, Government Services and Information Environment Group. With me are Mr Keith Besgrove - Chief General Manager, Regulatory and Analysis Group and Tom Dale - General Manager, Regulatory Branch.

NOIE's Role

NOIE:

Provides strategic advice to the Government on the key factors driving the information economy;

Facilitates information, knowledge sharing and, where appropriate, coordination of the application of new technologies to government administration, information and service provision, including online service delivery;

Promotes the benefits of, and Australia's position in, the information economy; and

Plays a key role in the implementation of the policy framework for e-security and authentication.

NOIE, and its preceding organisations, has played a leading role in creating whole-of-government attention to the opportunities that the electronic environment offers. Its focus may best be described as seeking to facilitate the transformation of government and business using information and communication technology as the key enabler.

As the lead agency in this space, NOIE has created frameworks (including facilitating the development of standards – for example, security and metadata, and Online Service Information Obligations) and tools (such as best practice information and checklists) to assist agencies as they make greater use of the electronic medium to capture, store and share data.

A key role fulfilled by NOIE is the capability to identify and bring issues to the table without a vested interest, enabling constructive considerations and facilitating the best possible outcomes.

A number of NOIE's initiatives have a direct relevance to the matters being considered by the Inquiry. NOIE has taken a lead role and worked with agencies in the development of policies and approaches to a range of areas including authentication, security and the provision of electronic information. Responsibility for implementation lies with the agencies themselves.

NOIE's Priorities

NOIE's 5 key priorities in the current financial year are to:

Promote e-security, facilitating implementation of a coordinated national e-security agenda;

Develop strategic advice on the demand drivers for Broadband and provide the secretariat for the Australian Broadband Advisory Group;

Encourage economic transformation through better information and communications technology (ICT) use across the Australian economy;

Transform Australian government information services and administration through the application of ICT;

Map the long-term uptake of e-business and e-procurement by small to medium business enterprises (SMEs).

Information Management Strategy Committee

Recognising the increasing use of ICT for government operations and its increased complexity, the Information Management Strategy Committee (IMSC) was created to provide shared leadership on multi-agency and whole of government information management strategies.

The IMSC is a collegiate body presenting a 'federated' model of information and communications technology (ICT) governance for the Commonwealth of Australia. Where appropriate, it acts as a reference body for government on governance of Commonwealth ICT. The IMSC is a leadership group that uses its influence to leverage support for approaches it develops.

The IMSC has no formal or statutory powers but if instances arise when it considers that formal authority is required to achieve desired outcomes, the IMSC will provide advice to the Minister for Communications, Information Technology and the Arts.

The IMSC serves as the principal forum for FMA agencies to:

share experiences and ideas to improve the management of ICT across the Commonwealth;

assess and address the human resource issues affecting the Commonwealth with respect to ICT management;

seek the views of other government committees at the Federal, State and local government level on matters of concern to the IMSC;

direct the CIO Council workplan and to consider proposals from the CIO Council;

provide shared leadership on cross-government information management strategies;

oversee the development of policies, standards, specifications and guidelines for ICT that will support business solutions for agencies while facilitating capacity for future interoperability;

identify and consider cross-government strategic information management approaches aimed to deliver whole of Commonwealth benefits, with a view to optimising the potential gains;

promote ICT investment, architecture and governance arrangements for strategic projects that support innovative business solutions;

initiate research and development into matters affecting whole of Commonwealth ICT activities; and

sponsor key strategic issues for ministerial consideration.

One of the priorities identified by the IMSC is to facilitate a trusted ICT environment. Important matters in this respect are secure government business systems and the authentication of clients.

NOIE provides support for the IMSC and the Chief Information Officer Committee (CIOC). The IMSC is a sub-committee of the Management Advisory Committee (MAC).

In its submission to the Committee, NOIE made a number of observations that, perhaps I can summarise.

Terms of Reference 1 - The privacy, confidentiality and integrity of the Commonwealth's electronic data.

Under the Privacy Act, the Financial Management and Accountability Act (FMA Act) and the PSM, the protection of information assets is the responsibility of each department and agency.

NOIE's role is to promulgate guidance and standards, to assist agencies and to facilitate synergetic cooperation between agencies and other parties.

NOIE encourages agencies to employ risk management processes in line with the PSM to assess and manage their risks and threats.

Terms of Reference 2 - The management and security of electronic information transmitted by Commonwealth agencies.

On this item, we made reference to:

Fedlink, a mechanism created to enable cost effective encrypted data traffic between participating agencies.

The Privacy Commissioner's Guidelines for Federal and ACT Government Websites.

DSD's Handbook 10 on Web Security that is part of ACSI 33.

The submission also noted that compliance with both the Privacy Commissioner's Guidelines and ACSI 33 was mandated by the Online Government Strategy, and agencies were required to comply with them by the end of 2001.

Terms of Reference 3 - The management and security of the Commonwealth's electronic information stored on centralised computer architecture and in distributed networks.

Variations in the configuration of an agency's network can have security implications but these can be managed within an overarching policy framework.

Similar general security policies and principles will apply irrespective of the network configuration, whether it be client server, or peer to peer, etc that is employed.

Terms of Reference 4 - The adequacy of the current legislative and guidance framework.

Elements of the legislative and guidance framework undergo periodic review in order to maintain adequacy.

Assessment of the adequacy of the current legislative and guidance framework will be part of the work of the IMSC and CIO Council.

NOIE's role in respect to this issue is to provide appropriate guidance, through seminars, publications and working groups, to help agencies understand and implement current legislative and guidance frameworks.

That concludes my introductory remarks. Thank you.

CHAIRMAN—In reading your submission, I was unclear as to the size of your agency.

Mr Grant—The size of the agency is approximately 190 including those people on term contracts. The number of full-time permanent employees is in the vicinity of 165.

CHAIRMAN—Gatekeeper is a Commonwealth government strategy for the use of public key infrastructure and a key enabler for the delivery of government online services and e-commerce issues. We have noted that, so far, the take-up rate for Gatekeeper seems to have been very low. Could you comment on that?

Mr Besgrove—I think it is fair to say that the take-up of Gatekeeper has been slower than may have been originally envisaged. In part I think that is because the take-up for public key infrastructure, both within Australia and within other countries, has been somewhat slower than people originally thought. Having said that, it is also fair to say that no-one has come up with a clear alternative to public key infrastructure and the persistence of interest in PKI around the world reflects the fact that it is still probably the best available set of technologies. Part of the reason why there has been some slowness in uptake has been the cost of implementation. Certainly the feedback we get from people is that they are waiting to see strong market demand before they commit.

CHAIRMAN—Do you think we overdesigned it?

Mr Besgrove—I will ask Mr Dale to comment on that. I do not believe that is really the issue; I think the issue has been more one of slowness of market acceptance. Australia's experience is not unique. I think it is fair to say that public key infrastructure has not taken off in other countries in the manner that some people expected it would. What we have actually seen is a fairly slow, albeit steady, set of implementations, predominantly in government and also in the banking sector. We are now seeing quite significant implementations, particularly in the United States government, but they have been happening only in the last 12 months; they certainly were not happening two or three years ago.

Mr Dale—The feedback that we have received both from industry participants and from Commonwealth agencies has been that Gatekeeper as a standard—which is all it is—has been not so much overdesigned; rather, assumptions were made three years ago or so about the growth of the PKI market, in both the government and the non-government sectors, and for a range of reasons those assumptions proved to be wrong. I think there is an interest in some greater flexibility within the existing Gatekeeper structure, but we have had no suggestion that it needs to be fundamentally taken apart.

CHAIRMAN—In their submission CSIRO said:

The gatekeeper guidelines ensure that organisations that wish to join this mesh conform to a useful and consistent standard, but it is also a prohibitively expensive exercise, with only the largest organisations able to compete. This seems

to be a costly duplication exercise for the Commonwealth Government and not consistent with a whole of government approach which would facilitate the uptake of PKI services.

Would you like to comment?

Mr Besgrove—I am surprised that they described it as 'prohibitively expensive'.

CHAIRMAN—Those are their words.

Mr Besgrove—I do not think that I can comment directly on those sentiments, because I have not had that sort of feedback myself. NOIE has been going through a process of consultation with stakeholders for the past year or so, looking at the whole authentication framework within Australia. As Mr Dale said, we have had quite a bit of feedback from people that is quite positive. It is certainly the case that a public key infrastructure implementation is not a costless exercise. One of the clear messages that has come out of our consultations is that the concept of fitness for purpose is very important. PKI is not necessarily the set of technologies appropriate for every purpose. For example, I presume you will be speaking to Centrelink in the course of these deliberations.

CHAIRMAN—Past tense.

Mr Besgrove—You have spoken to Centrelink. They, having looked at the needs and the benefits for their clients, have not gone down the PKI route. So at the end of the day our view has always been that PKI is something of a gold standard, if you like, and that there are situations where it is absolutely the right set of technologies to use, but it comes at a cost. The judgment as to whether it should be used by an organisation is very much a decision to be made by each agency.

CHAIRMAN—Would you mind having a look at submission No. 39 in this inquiry, on our web site, and coming back to us in writing with your view of its comments?

Ms PLIBERSEK—Eight organisations have Gatekeeper accreditation. That is out of what possible number?

Mr Dale—There is no actual number for that. The accreditation against the Gatekeeper standard is not for every agency using the standard. The accreditation is for the people or the entities that actually issue the certificates. There are a limited number of those who have expressed an interest for their own reasons, either commercial or otherwise. At the moment, that number of eight is not likely to change. That is just the number of people who believe there is a place in the market for them to operate against the Gatekeeper standard.

Ms PLIBERSEK—We had evidence from a number of organisations yesterday and some of them had partly taken it up. Was anyone appearing yesterday fully Gatekeeper accredited? I cannot remember.

CHAIRMAN—I think so. Tax was Gatekeeper accredited, wasn't it?

Mr Besgrove—Yes.

Ms PLIBERSEK—The impression some of the others gave was that, on top of the difficulties we have mentioned, they thought that the technology was just too difficult to use or would become obsolete in the not-too-distant future. Do you have a view on that?

Mr Grant—First, let us put Gatekeeper into context. It is a standard that, as Mr Besgrove said, meets the highest level of trust in dealing electronically between two organisations. Gatekeeper is not the only standard for this. If you look at the banks, for example, PIN and password work very well at this stage. Gatekeeper is a standard that is available where it makes sense. As more and more data is transferred electronically and you want to know that it is being sent securely and to the person or the entity that you think it is being sent to, then the likelihood of a greater requirement for the higher level of authentication is there. Obviously, it is also there where you require a signature. In that context, the framework for trust in the Commonwealth comprises the Gatekeeper standard; the ABN-DSC, which is a certificate structure where one certificate can deal with all agencies; and other mechanisms, such as the business authentication framework, which aims to provide a single gateway into the Commonwealth to provide those authentication services rather than each agency having to do it. In that context, we see the uptake of Gatekeeper as being less than expected but consistent with the demand from the market.

Ms PLIBERSEK—So you do not think it is a problem that it is less than expected?

Mr Grant—Not at all. I was going to use the example of the National Australia Bank and their online banking. They had a higher-level certificate than the other banks. Customers were finding it more difficult to deal electronically with the National Australia Bank. They looked at their risk and they went to the same level of authentication as the other banks, to retain customers and to provide that ease of access.

Mr Besgrove—If the uptake in Australia were slow—and it has been—and the uptake in many other comparable countries were much faster, we would probably have been concerned. In reality, the uptake in other countries has also been slow and in some respects Australia has been leading in some areas. The Australian Taxation Office, for example, is certainly a world leader in the use of digital certificates.

CHAIRMAN—Doesn't that tell you that maybe there is something wrong with it?

Mr Besgrove—That is not the conclusion that we have come to. The conclusion that we have come to is that sometimes markets take a while to accept new technologies and sometimes they take longer than people initially think will be the case. That does not mean that the technology is necessarily wrong or too expensive or too elaborate. It may mean that it will take some time for the market to recognise the value of PKI. But no-one is coming up with a serious alternative.

Senator LUNDY—What are the other forms of competing encryption technology that agencies and departments are using rather than going to the PKI solution?

Mr Grant—PKI is not just about encryption. It is actually about trust and authentication, with encryption as one of the elements. As you are aware, there are services such as FedLink, which provides encryption from router to router, and various agencies, depending on the level of data that is being transferred, may require some different levels of encryption. I do not have a list of what those different levels are.

Senator LUNDY—But they would not have a place for PKI—

Mr Grant—They may; that is just it. PKI is used where you are essentially dealing with someone at the other end of the line who you do not know and you wish to ensure, firstly, that the data is transferred securely and, secondly, that the data is transferred to where you think it is being transferred.

Senator LUNDY—But FedLink allows that to occur, doesn't it?

Mr Grant—It allows the data to be transferred securely router to router but not person to person. PKI is an individual based authentication—

Senator LUNDY—Why are some agencies deciding to only use FedLink? Why have they expressed confidence in that system and not seen the need to go to PKI as well? Is it because they already have confidence in it?

Mr Grant—No, it is because they either do not require that additional signature, which can assist in terms of responsibility and liability, or the level of the data they are transferring is not yet considered to be at a level where it requires the gold standard of PKI.

Senator LUNDY—How much of PKI's role do you estimate will be in department to department or internal government exchanges of information?

Mr Grant—I do not think we can estimate that. We do know that the HIC and the tax office at present have their own certifying authorities—they are PKI level activities, We know that the Department of Defence is looking at using that level of authentication for authenticating its own employees and dealing with agencies. Again, it comes back to the idea of fit for purpose and asking, 'What is the purpose you require it for?' And there would be a roll-out as a result.

Senator LUNDY—I am just trying to get my head around this; I do not really understand. If that is the highest level authentication and encryption technology and some agencies are choosing to use it but the rest are not—and, let us face it, a huge number are not—does that mean that in your view they are deficient in their security systems? Are they substandard or are they just choosing not to go to the highest standard because they do not have to and they cannot perceive a need?

Mr Grant—I think it is the latter. What they have done is reviewed the transactions they undertake and the dealings they have and, based on a risk assessment and the nature of transactions, they have said, 'At this stage, we do not need PKI.'

Senator LUNDY—So we have got a situation where most government agencies and departments think that PKI is too much security—that is, too much authentication and too much encryption?

Mr Grant—At this stage, it provides a higher level than they need.

Senator LUNDY—Is there any standard that mandates or insists that PKI be used? When does that situation occur?

Mr Grant—There is no standard per se but, if you have a look at the tax office, the tax office use PKI in dealings with 70,000 or 80,000 businesses and their accountants.

Senator LUNDY—I am talking about internal use in government at the moment. Is there any law, regulation or anything that says, 'PKI is the standard you must use'?

Mr Grant—No, there is not.

Senator LUNDY—My next question is to do with the relationship with external parties. Do you have any view on or estimate of the extent to which that could be used? Is there any regulation that insists it be used?

Mr Grant—Again, there is no regulation which says you must use PKI. It is a fit for purpose decision.

Mr Besgrove—Where Commonwealth agencies choose to go down the PKI route, the government has basically stated that they should be using Gatekeeper-accredited service providers.

Senator LUNDY—But they are not requiring that level.

Mr Besgrove—It is a decision to be made by each agency on the basis, as Mr Grant said, of their risk assessment, the nature of the transactions and what they regard as fit for purpose.

Senator LUNDY—Again, in the context of the Commonwealth dealing with external parties, what are the competing security encryption and authentication technologies that other agencies and departments use in communicating or exchanging information with external parties? What technologies are PKI competitors?

Mr Besgrove—We do not think of it in terms of direct competitors. We normally describe it as a hierarchy of technologies. So many agencies are using PIN and password combinations. I am not sure if agencies are using SSL.

Mr Grant—They are.

Mr Besgrove—There are a number of things. The banks use SSL—secure socket layer—technology, as the system for Internet banking.

Senator LUNDY—That is open source, isn't it? Isn't SSL freeware essentially? So agencies can use that.

Mr Besgrove—I do not know the answer to that.

Senator LUNDY—I am not sure either. It would probably be worth finding out. I presume departments and agencies would purchase PIN and password security software or it would be part of their software package.

Mr Besgrove—Presumably, but those sorts of technologies are pretty readily available in the marketplace. Each of those provides a level of trust that is, if you like, lower than PKI. The area where we see an emerging alternative to PKI is in biometrics, and we are doing a lot of work in relation to biometrics at the moment. The major difficulty is that there are no national or international standards for biometrics at this point in time. So the technology, while it is very promising, is in many respects very rudimentary.

Senator LUNDY—On the different levels of encryption, can you give the committee an insight into the ongoing debate in the technical community about the various merits of PKI versus other security software like secure socket layer? We were discussing it earlier. I know that there are several views that say there is no place for PKI—it is too much; it is over the top.

Mr Besgrove—I might ask Mr Dale to comment as well, but I would just make the observation that NOIE in its various roles has a lot of interactions with groups in other countries that are concerned with these issues. It is certainly the case that the US and Canadian governments are taking PKI very seriously and that some of the largest roll-outs in the world in PKI are being driven by the US government.

Senator LUNDY—In the last 12 months.

Mr Besgrove—Yes. So there is quite a substantial commitment on the part of those two governments, and we are starting to see more of that around the world.

Senator LUNDY—I am aware of that. Going to some of the technical aspects of comparing SSL to PKI, what is the level of encryption in those technologies respectively?

Mr Grant—We would have to get that for you. We are not technically conversant with the various levels. One of the things we have learned in our work is that quite often the encryption is fine for a variety of levels of information transfer. The difference arises in how the information is handled at the commencing of the transmission and at the end. That becomes a process issue, not a technical issue. I think it is a bit glib to say there is no place in the world for PKI.

Senator LUNDY—I am just reflecting comments in academia and other places in the technical community, because it is a debate you need to confront.

Mr Grant—My message to them, and I have said this to them already, is that PKI is there as a mechanism to provide trust, nonrepudiation—sometimes with other agreements—and liability. The others do not give that same level of responsibility for the transmission that is sent. So I think what we have seen is an overstatement of how quickly PKI will come on board. But as we have seen with many other technologies, ranging from video recorders to SMS on mobile phones, once it is understood and people actually look at their transactions and undertake that risk assessment, I would expect the uptake to be quite significant. The next part is where other facilitators in this area, such as biometrics, come in.

Senator LUNDY—Can you tell me what scope there is within the government, or for the administrator or the technical team supporting the PKI system, for the decryption of messages using the level of encryption that is used within PKI?

Mr Besgrove—I think we would have to take that question on notice.

Senator LUNDY—Would you provide the committee with a technical briefing on the operation of PKI, including the bit levels and the level of encryption, the process for decrypting messages sent via that system and the authorities associated with that.

Mr Grant—You are looking at the relevant standards for the sending and the receiving end?

Senator LUNDY—Yes, but also the level of encryption.

Mr Grant—Yes.

Senator HUMPHRIES—I would like to ask about the privacy policy. NOIE has a role in setting guidelines and standards in policy across agencies, but the agencies themselves have the responsibility to train their staff. Do you see yourself with a role in promulgating standards for training, such as the frequency of the training, and do you think that agencies are reaching that standard if there is such a standard?

Mr Grant—That responsibility lies with the Office of the Federal Privacy Commissioner, not with NOIE. No, we have not in the past set requirements for training and things like that.

Senator HUMPHRIES—Do you have an opinion about the appropriateness of the present requirements for privacy generally under the Privacy Act? If you had the capacity to modify those in some way, what would you recommend?

Mr Grant—I do not think we have a view on that; I think that is a question you should ask the Privacy Commissioner.

CHAIRMAN—Can you tell me how the frequently reported bugs, viruses and privacy breaches have affected public trust? Do you monitor that? It sounds like the kind of thing you ought to be monitoring.

Mr Dale—Yes, indeed. The responsibility for notifying federal agencies about those sorts of vulnerabilities—or in some cases attacks, but they are usually potential attack problems—lies primarily with DSD. We participate in a number of coordination bodies involving DSD, the Attorney-General's Department and other security and law enforcement agencies when particular issues such as new worms and viruses and so on are notified which are seen as being of particular concern. We participate in those bodies, and we might provide some advice and will certainly look at liaison with the private sector, but essentially the answer is that for Commonwealth agencies' security and protective action, which is often no more than simply downloading a patch, DSD use their network within the Commonwealth. As far as the private sector and the general public are concerned, the government relies on agencies such as AusCERT at the University of Queensland to undertake that role. I think that division of responsibility has over the last year or so seemed to work quite well as far as we can tell.

CHAIRMAN—Do you have any interaction with DSD?

Mr Dale—We have quite a lot of dealings with DSD.

Mr Besgrove—DSD are involved in some of the Gatekeeper accreditation work.

CHAIRMAN—It does not sound like that would keep you very busy.

Mr Besgrove—It keeps some of them quite busy; the process is somewhat involved. As Mr Dale indicated, we also have a lot of interactions with DSD through the various coordination committees that he referred to, and we also have an involvement with them through things like our annual bilateral discussions on security with the US government. So there is a range of interactions with DSD, and it is fair to say that we probably deal with them on a weekly, if not a daily, basis.

CHAIRMAN—CSIRO were not just unhappy with Gatekeeper. They commented that they were unable to subscribe to FedLink, because of the wide area bandwidth requirements. They found it too restrictive and their customers had difficulty understanding the need to use products endorsed on the DSD evaluated products list. Do you want to comment on that?

Mr Grant—I would have to follow that up with CSIRO. I find that an interesting statement in so far as FedLink provides encryption across a public network.

CHAIRMAN—I know.

Mr Grant—It provides a very cheap level of encryption for agencies and receivers. It is not actually meant for agencies dealing with the private sector.

CHAIRMAN—That is what I thought.

Mr Grant—It is for agency-to-agency dealings across jurisdictions. So that is an interesting comment by CSIRO.

CHAIRMAN—I would appreciate your comments, because I admit I was a bit surprised. I have one last brief thing on Gatekeeper. Do you have any idea of the costs to install it?

Mr Grant—You do not install Gatekeeper per se. It is a standard, and it allows for the accreditation of registration and certification authorities. Registration authorities look at evidence of identity checks and certification authorities allow the certificates to be checked for validity. In that context, businesses and, obviously, some government agencies have sought that accreditation. My understanding is that it is in the $300,000 range, but it may be more.

Mr Besgrove—I would not like to quote a bald figure of that sort. It depends upon the scale of the implementation and on whether you are seeking accreditation as both a registration and a certification agency or as just one or the other.

CHAIRMAN—Who would have a better idea than NOIE?

Mr Besgrove—We could get that information for you—

CHAIRMAN—Thank you.

Mr Besgrove—but I cannot give a figure off the top of my head today.

CHAIRMAN—That is quite all right. I am told by the secretariat that the committee discovered some of the submissions sent to this inquiry contained draft versions that could be accessed with a word processor's reviewing functionality.

Senator LUNDY—Through a track changes history.

Mr Grant—The process of accreditation is not based solely on documentary evidence. It is based on testing of sites and actual methodologies. That may be the case, but there is a thorough review of how the proposed system that goes with that operates. We are not aware, I might add, of a word processed document that anyone can pick up.

Senator LUNDY—I want to go back to PKI. You mentioned that there has obviously been a shift in attitude towards PKI by governments around the world over the last 12 months. Is that specifically linked with counter-terrorism measures and a heightened level of security? My understanding of PKI is that it does permit the authorities, if you like, to decrypt—presumably justifiably, if there is a security risk.

Mr Besgrove—I have had quite extensive discussions with the relevant people in the US Department of Commerce and also with relevant Canadian authorities. I have heard no suggestion from any of those people that counter-terrorism has played any significant role in the increased interest in PKI.

Senator LUNDY—But what about a general heightened level of security and far greater interest in IT security related issues in what is, generally, a heightened security environment?

Mr Besgrove—That is certainly impossible to argue with, Senator. That is pervasive across governments around the world today. But I do not believe that the US and Canadian administrations have a renewed interest in PKI because of counter-terrorism. Rather, I believe it has simply taken quite a while for those countries to get significant applications under way in a manner consistent with the experience of other countries.

Senator LUNDY—I am conscious of time. As NOIE has played a central role in providing support to many of the initiatives across the government, we may need to call you back at some later date.

Mr Besgrove—Okay.

Ms PLIBERSEK—I have a couple of very quick questions. Microsoft Australia and AUUG Inc. have made submissions. Microsoft states that there are security risks associated with open source software models and that they negatively affect industry development. AUUG states that open source software is the only practical way to ensure security, verifiability, interoperability and vendor independence. Do you have views about that debate?

Mr Besgrove—I think it would be a fair comment to say that those two submissions sum up well the state of debate in the market. NOIE's view is that there are clearly security issues on both sides.

Ms PLIBERSEK—Can you tell us a bit about the security issues on both sides?

Mr Besgrove—I might ask Mr Dale to comment in a bit more detail, but it is certainly the case that advocates of open source systems and advocates of proprietary operating systems each assert that the other has the greater security problems. It is very difficult to reach any sort of conclusion as to which is better or worse. It is clearly the case that both have security issues.

Mr Dale—I will give one example as far as government usage is concerned. If you were trying to establish accreditation for something like DSD's evaluated products list, for example, obviously there are going to be some serious practical issues to work through with evaluation of many types of open source software, which is almost continuously changing and, by definition, has no particular standard other than it has on a particular day. The experts in the government, primarily in DSD but also elsewhere, are certainly happy to look at that with an open mind. But I think, as Mr Besgrove said, the state of the debate on the security issue, as far as we can tell from monitoring it, is pretty much even at present. There is no one true answer coming through as far as relative security vulnerabilities are concerned. There are some practical issues, as I have said, and I am sure they will be worked through in due course.

Ms PLIBERSEK—I have one final question. In the past you have conducted online surveys, based on agencies' self-assessment, relating to privacy, confidentiality and integrity of the Commonwealth's electronic data. The last survey, round 4, is over a year old. Can you tell us briefly about those surveys—are they useful, and what information are you getting?

Mr Grant—The surveys were part of the online strategy. They were put in place, essentially, to assist agencies to review how far they had progressed in terms of addressing the issues that are identified as being important for an online presence and online transactions. We only ever proposed to do three, four or five surveys; we ended up doing four. I think the surveys enabled an agency to look at its progress and to see where perhaps more is required.

Ms PLIBERSEK—It is like a workbook, really.

Mr Grant—It was. What it has really shown us, though, is that, while not all the agencies made 100 per cent on every element, what they did is make huge progress towards that 100 per cent and dealt with areas that they might not otherwise have thought about.

Ms PLIBERSEK—Were there any areas of particular concern, where agencies were not getting it right?

Mr Grant—Of concern, no. We would have liked to have seen a higher percentage of completion in relation to some of the security areas—FedLink is a good example. The roll-out of FedLink has been a little bit slower than we might have expected, because agencies have to get their internal processes in place—the technology is there but the processes are not. It is not an easy thing to do and it is not an inexpensive thing to do. That is what agencies learnt as they went through the process of reviewing their progress.

CHAIRMAN—Does NOIE have a CIO?

Mr Grant—I do not think we have a CIO per se. We only have a very small IT requirement—it is basically desktop and a few databases.

CHAIRMAN—Were you involved in the production of the document entitled *Australian government use of information and communications technology: a new governance and investment framework*?

Mr Grant—Yes, we certainly were.

CHAIRMAN—Do you agree with all of that?

Mr Grant—Yes.

CHAIRMAN—Then what more can I say. Thank you. If we can ask our questions in writing instead of getting you back, you would not mind responding to that, would you?

Mr Grant—That is not a problem at all.

CHAIRMAN—We will see how we go. Thank you very much for your cooperation.

[10.18 a.m.]

WHITTAKER, Ms Sheelagh, Executive Vice President, EDS Australia

CHAIRMAN—I welcome the representative from EDS. We thank you for your submission, which we have published. Do you have a brief opening statement or may we start to ask you questions?

Ms Whittaker—I have a very brief opening statement. I am responsible for EDS's federal government business. As an outsourced service provider, EDS is concerned not only with delivering services cost effectively but also with delivering high-quality services to our clients. It is a commercial reality that, were a company like EDS to deliver services focused purely on cost minimisation, we would neither satisfy our clients nor deliver to them any long-term strategic business value.

EDS is totally committed to meeting our information, security and assurance responsibilities by supporting and applying the government's information privacy, security and integrity assurance policy framework, structured around the *Protective Security Manual*, the Australian communications electronic security instructions, the Privacy Act, the Gatekeeper strategy, the Australian business number digital signature certificate and FedLink.

From Customs' operational implementation of closed-system, limited-access architecture to the ATO's strategically focused and organisationally aligned approach to the management and protection of Commonwealth information, EDS is committed to the support of department-specific approaches to information protection within a whole-of-government framework. EDS works with customers in the ATO to achieve effective management and protection of the information in their care.

Above all, it is important to recognise that, regardless of the differing policies or technologies and operational or strategic approaches, risk, risk assessment and mitigation are at the core of information protection. Risks cross the boundaries of technology process, business methods and practice. Risks develop and change continually. If I were to leave you with one thought today, it would be this: risk is not a static concept; as a result, we must all be constantly and flexibly vigilant in the identification and mitigation of risks across technologies, business processes and business interfaces.

CHAIRMAN—In your submission, you advocate single source outsourcing arrangements. Can you, firstly, tell us why single point outsourcing will facilitate management integrity of our electronic data and, secondly, answer how you think it is going to increase competition when, in fact, it will reduce the number of competitors who are able to play?

Ms Whittaker—What I advocate in our submission is that, in order to effectively play the stewardship role—which is an increasing role—in the protection of the government's information and information security, you need a single throat to choke. It can be an internal agency or an external contractor. But the proliferation of various different service providers without one single point of accountability increases the risk that the government faces in its information security management.

CHAIRMAN—You did not answer the restriction of competition question.

Ms Whittaker—I do not believe that the prime contractor or contract office model necessarily restricts competition. We are not suggesting fewer suppliers; we are suggesting a modality of contracting which gives the government a single point of contact. So there will not be fewer suppliers; there will just be a more clear-cut relationship.

CHAIRMAN—Perhaps I am a little confused. The government has worked hard over the last few years to try and get information about its purchasing and contracting requirements in electronic form and to give the business community constantly increasing access to what the government's purchasing and contracting requirements are. You want to go back to a single point, so that all businesses in Australia that potentially want to do business with the government electronically need to go through a single gateway?

Ms Whittaker—No, that is an oversimplification. I am sorry if I led you to believe that that is what we were suggesting. What we are suggesting is that each department or agency has a role as custodian of the information that it holds in trust for the government and it, in turn, needs to have a steward who will manage the security aspects of that set of information. That steward may be an internal contracting agency within the department or a contractor to whom the department has given that responsibility. The focus here is on the control, security and integrity of the information that the department is the custodian of. So it is about information security—it is not about procurement.

CHAIRMAN—What obligations does EDS have to protect the security, privacy and integrity of the government's electronic data?

Ms Whittaker—We have contractual obligations with the customs office and the Taxation Office. They are stringent. We have service level agreements inherent in those contractual obligations. Constant auditing takes place of our performance of those contractual obligations.

CHAIRMAN—Can you tell me why you have not applied for Gatekeeper?

Ms Whittaker—I am not sure what you are asking.

CHAIRMAN—Gatekeeper is the government's strategy for public key infrastructure for delivery of government online and e-commerce. It would allow you to authenticate data sent electronically from government agencies. NOIE says that you have not applied for Gatekeeper certification.

Ms Whittaker—No. As the NOIE representatives explained, Gatekeeper is a certification function. Often my colleagues in businesses like audit apply for that kind of certification function. In fact, if we were a gatekeeper, it could lead to a potential conflict of interest, because we would often want perhaps to be certified. If you are the certifier and are applying to be certified, it could lead to potential conflict of interest.

Senator LUNDY—Are you certified as opposed to a certifier?

Ms Whittaker—In those instances where we wish, for example, to use PKI, we are certified as differentiated from being a certifier.

CHAIRMAN—I thought that FedLink was for communications between government departments and Gatekeeper was the gate through which communications flow to and from external providers and it provides a reasonably secure guarantee that people and organisations are who they say they are when you are dealing electronically—it authenticates both signatures and authority.

Ms Whittaker—I could get back to this, but it is my understanding that the gatekeeper is the certifier. Can I follow up with the committee about clarification on this point?

CHAIRMAN—Yes, sure.

Ms PLIBERSEK—It does not say anywhere in your submission what EDS stands for and I do not know off the top of my head. Could you tell us?

Ms Whittaker—It stands for Electronic Data Systems.

Ms PLIBERSEK—That is the name of your company as well as a description of what you put out?

Ms Whittaker—Over time, our company has evolved from calling itself Electronic Data Systems to EDS, in the fashion of three-letter acronyms.

Ms PLIBERSEK—I think the main point of your submission—as well as the single-source outsourcing point—is about developing a role for the stewardship of information. Do you want to talk a little bit about what you see as that role and how it would be enforced?

Ms Whittaker—Yes. Stewardship first of all needs clear definition. It needs to be understood that, either on a contractual basis or internally—if it is an internal function on a contract management basis—this particular function is responsible for managing and protecting and ensuring, in an iterative sense too, that the information is secure and that information integrity and information assurance processes take place. Those can be stipulated. They are now stipulated in various ways in contracts, but there is a body of expectation that can be common to the performance of the role across all stewards in all departments and agencies. We are suggesting that, perhaps, there could be a clear recognition that stewardship must take place and a clear recognition that it involves a certain list of activities or behaviours.

Ms PLIBERSEK—When you talk about clarity in that role, do you mean that government information technology contracts should be standardised to include a model description of the role of the steward? What are you talking about in terms of standardisation?

Ms Whittaker—It would not be a bad idea to have a small standardisation in all contracts about the role of the steward. I am thinking here about levels—

Ms PLIBERSEK—What would it say? If you were writing the contract from the government's perspective, rather than your own, what would you say?

Ms Whittaker—It would have to do with stipulated levels of security clearance required for certain kinds of functions. It would have to do with internal and external audit requirements of security performance. It would have to do with monitoring, safeguarding and assessing, where appropriate, whether there is the need for things such as PKI—that is, certification issues. It would set standards for the stewardship of the information.

Ms PLIBERSEK—Do you think that that is not written into contracts now?

Ms Whittaker—It is, but it is written in variously, and there is no common standard for stewardship.

Ms PLIBERSEK—Do you think it is written in adequately in most contracts?

Ms Whittaker—Generally, yes, I do.

Senator LUNDY—I want to talk about the issue of contractual responsibility. Is it possible for agencies and departments to effectively contract out their responsibility for security?

Ms Whittaker—No.

Senator LUNDY—So how can you, as the steward, say that that is effectively what your value proposition is as a company?

Ms Whittaker—No, I am saying that the agency is the custodian of the information. It holds the information in trust for the information owner, who is in this case the citizen, and it looks after that information, on behalf of the citizen, for the use of all the parties who have legal access to it. In this case, their way of exercising their custodian function is through the steward, who is an expert or who is expected to be an expert in that particular process. That expertise can be vested in the agency or it can be vested outside, and I am proposing that the government ensure that that expertise—the capability to effectively execute the steward role—exists, either inside or outside the agency.

Senator LUNDY—I liked your description earlier of having one throat to choke. My experience with large IT-outsourcing contracts, like the ones EDS have with both Tax and Customs, is that it is not possible for the Commonwealth to not be the throat to choke. It is accountable to the people and the parliament. So there is a limit to which that responsibility can be effectively transferred to a contractor or to a steward, as you describe it. I want to explore the nature of the contractual obligations that you have, particularly in relation to sanctions. How would they apply if, in fact, you failed to meet some of your service level agreements relating to security, for example? What do the contracts actually provide for if that were to be the case? My understanding is that those contracts do have sanctions in them and that the sanctions would be applied. But, other than that, nothing else happens. Your contract is still in place. You pay a financial penalty as a company, but nothing happens beyond that. Can you comment on that and confirm whether or not my reflection is accurate?

Ms Whittaker—Of course, the ultimate sanction is non-renewal, and the possibility of that is always there.

Senator LUNDY—Is that a possibility if you fail on your service level agreements in relation to security? At what point does it become a threat to your contract? How high a security breach does it have to be? Because my experience with all the IT outsourcing contracts is that there is no sanction or breach in sight that has come anywhere near to an agency or department being in any position at all to remove itself from the contract on those grounds.

Ms Whittaker—In the day to day operation of our contracts the service level sanctions are routinely financial penalties. However, for example, both contracts we have right now are only for a duration of two years, and the refusal to renew can be for any reason. So the ultimate sanction of non-renewal is never very far away. And both parties are aware of that. So on a day to day basis there are the service level agreements, the financial penalties—which are onerous; they are non-trivial financial penalties—and then there is, as I have said, the ultimate sanction of non-renewal.

Senator LUNDY—I guess I am very sceptical about the non-renewal, because of a whole range of issues. Firstly, there is no evidence at all through a series of inquiries that demonstrates that many sanctions have occurred—many breaches of service level agreements have occurred. From memory, the responses I have had from departments is that they—and I think it was DCITA reflecting on the nature of the contracts—do not believe that non-renewal of contract is a realistic option if, say, an industry development commitment was breached. How many sanctions have been applied to EDS on security related issues?

Ms Whittaker—Off the top of my head I cannot think of any, but I will look into it and see if there have been any security related breaches and I will provide you with that information.

Senator LUNDY—We have heard from agencies and departments that they use the ISIDRAS reporting system with DSD if they report incidences of attempted hacking or penetrations by viruses and worms et cetera. Does the notification of DSD lie with the department or agency or with EDS as the primary contractor?

Ms Whittaker—EDS has a global threat vulnerability monitoring, TVM, system. In two recent instances that have been very high profile that system has safeguarded our customers. In the case of the Melissa virus, which first manifested itself in North America, we were able to advise our customers here and close the gateways so that the virus did not have an impact on our customers. The Slammer was actually detected by our team in South Australia, who were responsible for not only informing our customers in this country and isolating the servers that could have been impacted but informing the world of the Slammer virus.

Senator LUNDY—Did you have the patch in place before Australia Day this year for the SQL Slammer bug?

Ms Whittaker—We were the ones that identified the SQL Slammer.

Senator LUNDY—So you had the patch in place?

Ms Whittaker—We had the patch in place. But, speaking of patches, I think you should understand that in our kind of business we routinely look at lists of patches that come from the suppliers and apply them proactively. We do not wait until there is a threat. If a software supplier tells us that there are patches, we apply them.

Senator LUNDY—I understand that Microsoft software is used extensively in Tax. Do you describe Microsoft as being an EDS partner in the solution you provide to the tax office?

Ms Whittaker—Insofar as we provide side by side within Tax, our job as a systems integrator in the world is to work well and effectively with all other hardware and software suppliers so that the customer gets the best out of the relationships.

Senator LUNDY—I want to go back to the issue of security breaches again. Government employees, public servants, can be sent to jail if they are found guilty of a security breach, but can you confirm that under your contract if a private company—in this case, perhaps yours—is responsible the only sanction available to the department or agency of government is a financial penalty?

Ms Whittaker—Our employees are, of course, security cleared, where appropriate, by the government, so the removal of security clearance is a sanction open to the government. From our perspective, you can well imagine that those employees do not continue to have employment.

Senator LUNDY—For individuals, the law is quite harsh. I guess what I am seeking confirmation on is: if EDS as a company were found to be responsible for a security breach—say, a technical issue that you were contracted to ensure was secure and so on—is there any sanction available in those contracts other than a financial penalty?

Ms Whittaker—I would have to check that with our corporate counsel. Could I provide that answer in writing to the committee?

Senator LUNDY—Yes, thank you.

Senator HUMPHRIES—I want to ask a general question. You talked about risk and emphasised that it was not static. What do you see as the key risks facing Commonwealth electronic data management in the next couple of years?

Ms Whittaker—As I said, we have our global threat vulnerability and monitoring system because there is constantly the risk of various manifestations of hacking. The issue with the Slammer virus was that it was a risk against servers; previously, viruses and bugs had affected software instead of hardware. I would say that the greatest risk is in looking backward at what the previous risks have been and protecting against those, as differentiated from looking forward and having people whose responsibility is to hypothesise new and different kinds of risks that might manifest themselves and how we would guard against those.

Senator HUMPHRIES—You mentioned that EDS had been responsible for verifying the Slammer virus and disseminating the warning about that. Is there enough information sharing at that level between private sector companies themselves and between private sector companies and government in identifying the sort of risks that you are talking about?

Ms Whittaker—What interested me was that EDS took some pride in having informed the FBI of the Slammer virus. From an Australian point of view, we are not as closely integrated in, say, the DSD or equivalent infrastructure of Australia where we would automatically inform an equivalent. We inform our customers, who in turn inform DSD. Because of the homeland

security issues and because of the fact that the American government has brought the industry closely in to worry about and deliberate on issues of security and data protection, it seemed to me that there was perhaps a tighter relationship there between government and business. Having looked at that, I wondered on Australia's behalf if we ought to have a tighter connection too.

Senator HUMPHRIES—EDS has non-government customers, I assume?

Ms Whittaker—Yes, we do. Two high profile customers are the Commonwealth Bank and the Westpac Mortgage Processing Centre.

Senator HUMPHRIES—How do your staff training requirements differ between your private sector and public sector clients?

Ms Whittaker—We have a standardised, online, must be certified that they have taken it, security course for all EDS employees. Tax and Customs have supplementary standard training for security that our employees must take. Different organisations supplement our standard security training with their own expectations, but I think the Commonwealth's expectations are very high in this regard.

Senator HUMPHRIES—Appropriately high?

Ms Whittaker—Yes, appropriately high.

CHAIRMAN—Thank you very much for coming and talking to us today. If we have further questions, you will not mind if we put them to you in writing; will you?

Ms Whittaker—No. Thank you.

Proceedings suspended from 10.45 a.m. to 11.02 a.m.

CUNNINGHAM, Mr Adrian Edward, Director, Record Keeping Standards and Policy, National Archives of Australia

DAN, Ms Kathryn Patricia, Assistant Director-General, Government Record Keeping, National Archives of Australia

STUCKEY, Mr Stephen John, Acting Director-General, National Archives of Australia

CHAIRMAN—I welcome representatives of the National Archives of Australia to today's hearing. We thank you for your submission, which we have published. Do you have a brief opening statement?

Mr Stuckey—Yes, I do.

CHAIRMAN—When I ask that, I mean really brief.

Mr Stuckey—It is brief—a couple of paragraphs.

CHAIRMAN—Terrific.

Mr Stuckey—The National Archives thank the committee for the opportunity to appear before you and answer your questions. As the Commonwealth's record keeping authority, we have a major interest in the management and integrity of electronic information in the Commonwealth. One of the main objectives of the archives is to promote good record keeping in the Commonwealth. A particular priority for us in recent years has been assisting Commonwealth agencies to make and keep accurate, reliable, authentic and secure electronic records. We do this by providing expert advice, assistance and training to agencies on strategies for pursuing the best practices in this area.

Evidence from a variety of sources indicates that record keeping in the Commonwealth is in a parlous state and that agencies need guidance to help them manage the transition to full and accurate record keeping in the digital age. While we feel that we are making some progress with our objectives in this area, convincing senior managers in agencies to take the issue seriously nevertheless remains a significant challenge.

One issue that we have identified as a strategic hindrance to the Commonwealth in the pursuit of sound electronic record keeping regimes is the absence of a coherent, overarching information management strategic and policy framework. We feel that it would be of great benefit to the Commonwealth if the National Archives permanent record keeping policy framework could be articulated and progressed within the context of a whole-of-government information management framework that has high-level mandate and support.

CHAIRMAN—In your submission, you mentioned the May 2002 ANAO report *Assurance and control assessment audit: recordkeeping*, which looks at record keeping in four Commonwealth agencies. The report found that the agencies are in a state of transition and none fully satisfied the audit criteria. Can you tell us a bit about that report?

Ms Dan—Certainly. What the Audit Office found in looking at that selection of agencies was, as we said, a state of transition. Many agencies were moving from a situation where they had well established practices for dealing with paper records and staff with training and knowledge in those areas to a situation where it was really a blank slate and they did not have policies, frameworks or established procedures. So many of them were struggling with the transition. Essentially, the audit report found gaps in what people were doing and, I think significantly, disintegration in a strategic view of management of information. Many agencies were doing many things, but in a siloed way across the agency. So, for example, they might be implementing an electronic document management system, they might be doing some work in relation to our standards about record keeping, they might be upgrading their business IT systems, but they were doing many of those things in isolation, without bringing them together in a strategic sense.

CHAIRMAN—Do you have a CIO?

Mr Stuckey—Within National Archives?

CHAIRMAN—Yes.

Mr Stuckey—Yes, we do.

CHAIRMAN—Did the National Archives participate in the preparation of a document called *Australian government use of information and communications technology: a new governance and investment framework 2002*?

Mr Stuckey—No.

CHAIRMAN—Have you read the document?

Mr Stuckey—Yes.

CHAIRMAN—Do you believe that implementation of some, at least, of what that Management Advisory Committee document commits to would lead towards the kind of outcomes you are looking for?

Mr Stuckey—Yes, we do. There are a lot of recommendations in that report, and it will be expensive for government to implement all of them, but an acknowledgment of the framework is the first step and then chief executive officers of agencies must understand the need for the coherent approach that Kathryn Dan was talking about.

CHAIRMAN—Can you tell us a bit about disaster recovery and how that fits into where you see electronic record keeping future strategy?

Mr Stuckey—Disaster recovery is just part of good housekeeping of information. Generally, and regrettably, in both the public and the private sectors it tends to be a priority after the event—that is, when you realise you cannot recover and you then understand how good or otherwise your disaster recovery plans are. The Audit Office is in the process of doing a select audit across the Commonwealth about the security of electronic information, and we have the

honour to be one of the agencies that is being audited in that regard. Our view is that, as the advisers to the Commonwealth about these sorts of things, our own procedures need to be good.

CHAIRMAN—Are they?

Mr Stuckey—They have not been tested yet by a disaster, but we think they are. An internal audit last calendar year picked up some gaps, but it is something that generally the IT industry and IT managers within Commonwealth agencies are conscious of. It is in all the literature; therefore, it is the sort of thing you can run a checklist on—that is, do we do this; do we do that? As an example of something we are doing, we keep part of our mainframe computer in the National Library's computer suite and they keep some of theirs in ours, so they are separated, at least in this city, by a kilometre, and backup tapes for us are in the National Library and vice versa. So it is the sort of thing that IT managers give attention to.

CHAIRMAN—If I owned a private company and held all my tax records, which are all paper based, in a warehouse and the warehouse burned down, I would have some difficulty with the tax office proving or disproving anything in the future. Would you say that we are really in worse shape than we were when we just had paper based systems? I certainly would not have backed that up in any way.

Mr Stuckey—Probably not from a disaster recovery perspective. One of the lessons learned from the attack on the World Trade Centre in September 2001 was that certain corporations lost their paper records but they had electronic data backed up offsite and were able to recover some of that data. One of the advantages of the IT industry is that it is easier to back up than to photocopy or microfilm, for example.

CHAIRMAN—So you are not critical of the e-commerce world but what you are saying is that we need a management plan on how to manage it and how to do it more uniformly than in a disaggregated way. Does that summarise it?

Mr Stuckey—Yes.

CHAIRMAN—CSIRO says that record-keeping strategies, like your e-performance standards, are often 'couched in theoretical terms with little practical advice'. It also states that the government online strategies 'conflict with the practical requirement of agencies'. Would you like to respond to that?

Mr Stuckey—CSIRO is not the only agency that has said to us that it needs more practical advice, and we are giving practical advice. But in defence of both our strategy and the wider government strategy, I think you need to articulate the principles first and then work out how you best implement them. We have had the theoretical advice out there now for three years. It is in the process of a major review because a lot of agencies in the government are implementing it and have said to us that it needs to be more flexible and that there needs to be more practical advice. It is still relatively new territory, partly because of the disaggregation and the fact that the IT intrusion, if I can call it that, within public or private sector business has not been a big bang; it has been incremental. I think our processes are catching up after the event.

CHAIRMAN—You would not really want us to go back to a centralised command authority, would you?

Mr Stuckey—In implementing government and agency rules about how you deal with information, that is exactly what we are saying. In the dealing with any other asset, whether it is money, people or buildings, there are government guidelines on how you, say, spend taxpayers' money. There need to be central guidelines on the principles that you apply for managing a huge asset.

CHAIRMAN—A guideline is a bit different from a central command authority.

Mr Stuckey—We do not want a central command authority. That would not work in a devolved business world.

Ms PLIBERSEK—Can you give us an outline of the e-permanence suite of best practice record-keeping standards manuals and guidelines? Can you give us an overview? We have not looked at them.

Mr Stuckey—I am not surprised—there are more than 2,000 pages! One of my technical experts can deal with that better than I can.

Mr Cunningham—The starting point for the suite of guidelines is in fact the Australian—and international—records management standard ISO 15489. That was published about a year ago and actually was based on an earlier Australian standard, from 1996—the world's first records management standard, in fact.

Ms PLIBERSEK—We had the world's first one?

Mr Cunningham—We did, in 1996.

Ms PLIBERSEK—Who was responsible for that?

Mr Cunningham—It was a collaborative effort, but the National Archives was one of the collaborators. The rest of the world liked it so much that they adopted it as an international standard, with some revisions and improvements. That was a feather in Australia's cap. When the original standard was issued in 1996, it was obviously a high-level document, meant to apply to organisations from a corner florist right through to the Department of Defence. It was fairly general in that sense. We realised that, in terms of translating that general advice into something more detailed for Commonwealth agencies to make good use of, we needed to develop a suite of more detailed products and guidelines based on that international standard. That is effectively what the e-permanence suite is.

The foundation of the suite of products is the DIRKS manual, which stood originally for 'designing and implementing record keeping systems'. It is an eight-step process that organisations can undertake to assess their record keeping requirements and judge their existing systems and practices against their identified requirements and then develop and implement strategies to, if you like, fill the gap between the current performance and the identified requirements. It is a strategic approach, and really everything else in the e-permanence suite of guidelines hangs off the DIRKS manual in one way or another. It sorts of picks up an aspect of the DIRKS methodology for a particular outcome or whatever and extrapolates that in more detail.

For instance, one of the other products we have in the e-permanence suite is a set of policies and guidelines for the archiving of web based resources. Effectively, that takes the DIRKS methodology and applies it to a particular category of electronic resource, a particular outcome, that organisations are looking for. Another key product in the suite is a record-keeping metadata standard. Metadata is the information within record-keeping systems that makes the systems work, in effect. It is the information that the systems have to manage. When systems designers are designing a new record-keeping system, one of the questions they need to answer is: what is the metadata that the system is going to make and keep? Our metadata standard helps to answer that question for them.

Ms PLIBERSEK—I do not really understand that. Can you tell me that in another way? Explain what metadata is.

Mr Cunningham—Metadata is just information about other information. If you have a body of records that need to be managed, you need to apply an information regime to that body of records so that information within that group of material can be found if it is needed, so that it can be understood when anyone wants to look at it and ask: 'Why was this created? Who made it and when? Who used it and when?'

Ms PLIBERSEK—And also for people to ask, 'How often has it been amended?' and that sort of thing?

Mr Cunningham—Yes, and also for them to ask things like: 'Was it disposed of? When? With what authority?' All that is the sort of information that is absolutely critical in a record-keeping system. For shorthand purposes nowadays we call it metadata. Standardising the metadata requirements for record keeping is a fairly critical thing to do and, by issuing a standard in that area, we hope to save agencies the trouble of having to reinvent that particular wheel.

Ms PLIBERSEK—Has there been a high uptake of your standard by agencies?

Mr Cunningham—There has been a very high uptake of the DIRKS manual; a large number of agencies are implementing the DIRKS methodology now. The reason for that high uptake is that we have made the adoption of the DIRKS methodology conditional for us issuing agencies with disposal authorisation, which is one of the powers we have under the Archives Act. No Commonwealth record can be disposed of without our authorisation. We now say to agencies, 'If you want our authorisation you have got to at least make a start on the DIRKS process.' So that has been an encouraging level of uptake.

I would say, though, that the metadata standard is less well known and less well appreciated—I think we have still got more work to do in terms of communicating its role in the landscape. I suspect that that lack of uptake is probably a reflection of the fragmentation of efforts which we have referred to. Quite often, a DIRKS project in an agency will be conducted by a records management unit and at the same time there will be an electronic document management project operating in an IT area in that agency; the two groups of people do not speak to each other and the IT team that is doing an EDMS project will not even be aware of Archives' guidelines in this area. So we need to keep doing more work in terms of raising our profile with non-traditional audiences, if you like.

Ms PLIBERSEK—Are the metadata standards that you talk about only relevant at the time of the design of a system? Or do people go back later and add to or change the metadata that their system records?

Mr Cunningham—It is relevant at both points. One of the aims of good record-keeping systems design is to have clever systems which are self-documenting as much as possible so that the end user does not need to worry about what metadata they have to create; the system, in effect, does it for them. But obviously there are limits to how much clever systems can achieve in that area. You cannot take human beings entirely out of the equation. The audience for our metadata standard is obviously not the average public servant; it is systems designers. But, ultimately, the average public servant would be aware of metadata to the extent that if they were asked to populate a field in a template or whatever with a piece of information then in effect what they are doing is creating metadata. One of the things we try to emphasise to agencies is that once you decide what metadata your system needs to capture and once you have worked out what metadata has to be created by a human being then you should try and make it as easy as possible for them to do that and give them the requisite training, policy guidelines and so forth.

Ms PLIBERSEK—You have got a paper coming out soon on the record-keeping implications of the use of authentication and encryption processes and technologies?

Mr Cunningham—Yes, we do.

Ms PLIBERSEK—Can you tell us a little bit about that?

Mr Cunningham—Yes. Just a couple of days ago the paper reached external consultation stage. We have notified a wide range of external stakeholders that we have this exposure draft, and we will send it to anyone who asks to have a look at it.

Ms PLIBERSEK—Would you mind sending it to our committee secretariat, just out of interest?

Mr Cunningham—Sure. The aim of the guidelines is to ensure that both short- and long-term record-keeping requirements in relation to the use of authentication technologies are acknowledged by agencies and dealt with appropriately. One of the things we are concerned about with the uptake of new technology is that in the rush to adopt the new technology the record-keeping issues get overlooked. This is a classic example of us trying to give agencies a bit of a heads-up and saying, 'You might be adopting PKI or some other kind of authentication technology, but please don't forget these particular issues to do with record keeping.'

Ms PLIBERSEK—And what are the issues?

Mr Cunningham—One of the main ones is ensuring that the information that needs to be retained is retained, and is accessible and comprehensible, for as long as needed. We are talking 10, 20, 30 years or longer in some cases.

Ms PLIBERSEK—So you are worried that the technology will change and make it difficult to decrypt the information, or are you worried that passwords will get lost and the human element will make it difficult to access the information?

Mr Cunningham—All of those things are of concern to us. For instance, if business critical records are stored in an encrypted form and the key gets lost or the authorisation expires after, say, three years but the record is still needed after five or 10 years, obviously the Commonwealth has a problem. The aim of the guidelines is first of all to alert agencies to this potential problem and then to give them some practical guidelines as to what they can do about it.

Ms PLIBERSEK—In the writing of this paper have you had a chance to look at how agencies are dealing with this issue so far and has it given you cause for concern?

Mr Cunningham—We certainly have had a chance to look at what agencies are doing. In particular, we have had some very fruitful contact with agencies like the Health Insurance Commission, the Australian Customs Service and the Australian Taxation Office, all of whom have been at the forefront of using authentication technologies. It has been useful for us to find out what agencies are actually doing and about the sorts of implementation strategies and objectives they have and to then talk them through some of the record keeping issues. The agencies have found it useful to talk to us, but we have also found it useful to get our heads around the issue and frame up what we hope will be quite useful advice for agencies.

Ms PLIBERSEK—Are any of them indicating that they are going to change their practice after discussions with you?

Mr Cunningham—Yes. The few agencies that we have had direct dealings with so far have been very attentive to the sort of advice we have given and we have found it to be a very constructive relationship. We have also obviously been talking with the National Office for the Information Economy, who set the general government framework for this. They have incorporated some of our advice into their general guidelines and also suggested to us the desirability of working with Standards Australia to develop a version of this advice for private sector application as well, because obviously it is not just the public sector that is concerned about these issues.

Ms PLIBERSEK—So what sorts of steps can organisations take to deal with the concerns that you have raised? Do they leave the key somewhere? What do they do to prevent this information becoming inaccessible over time?

Mr Cunningham—Firstly, the records pertaining to the operation of the keys themselves have to be managed very carefully. The records dealing with the issuing of keys, the maintenance and use of keys, who has authorisation to do what and when and so forth have to be very carefully created and managed and they have to be accessible for as long as the information is likely to exist. One of the potential strategies as well is—we cannot make a blanket rule about this—that as a general guide we say to agencies that it is probably not a good idea to store their records in encrypted format. There are exceptions to that of course but, as a general rule, we think encryption is best used for transmission purposes, not for storage purposes. Security concerns ought to be able to be addressed through means other than encryption.

Ms PLIBERSEK—Are many organisations currently storing information in encrypted form?

Mr Cunningham—I do not have enough information to give you a good answer on that. I am sure that some are, but how common the practice is I am not sure.

Ms PLIBERSEK—I have one more question about long-term preservation and secure storage of digital Commonwealth records that we might want to have a look at later. You mentioned the Health Insurance Commission, and I can understand why researchers in 30 years time might be very interested in looking at those records. You have announced an archives to researcher digital preservation project. Can you tell us a bit about that?

Mr Stuckey—I can probably talk to you about that. One of the guiding principles for us has been that we are not going to lock the Commonwealth into relying on proprietary software. If you are creating stuff in Microsoft 2000, or Microsoft 2008, when those records become publicly available in 2040 we do not want the Commonwealth still to be paying licence fees to Bill Gates for Microsoft 2008. The chances are Microsoft will not support that sort of software. That was a guiding principle when we set out to work out how we were going to solve the problem.

We decided that we had to go to open office software, and we were criticised, both within this country and internationally, for holding fire about what we were going to do about preserving digital objects for some years. There were places overseas that jumped in and said, 'We will rely on this software.' Our view was that time would ensure that open sourceware would be demanded by the users, and that has indeed happened. We are therefore relying on XML, extensible markup language, which in effect captures the zeros and ones which are the digital objects. It manages them in such a way that they are software independent.

Ms PLIBERSEK—So you can read them no matter what system you are on.

Mr Stuckey—Absolutely. What you do need, though, is a filter. You need to design a filter that will say, 'This series of zeros and ones is the letterhead of the Prime Minister and this is what it used to look like. This set of zeros and ones is the words that were on the letter. This series of zeros and ones is the encryption.' We have developed a software package within the National Archives in the last 18 months. They are all cutely named, and ours is called Xanadu.

Ms PLIBERSEK—Does it stand for anything, or is it just a flight of whimsy?

Mr Stuckey—It is just a bit of whimsy, really. Sometimes IT people can be creative. We will release that on our web site in July, and it will be freely available to anyone around the world. It captures documents in their native software, whether that be Microsoft or Apple Macintosh. It captures the zeros and ones, identifies what they are and stores the original zeros and ones, because for evidentiary purposes we need to be able to come back and say, 'This is what it really looked like, if you have the software to read it.' But we put the other zeros and ones through the XML filter into a digital repository, and we can then create an emulation of the document. We are assuming that that software will always be freely available, because it is in the national interest that it is. I hope we would be able to resist the blandishments and the large financial offers that might come forward to buy the IP. We made that decision as the only way we could keep that stuff authentic and independent.

Ms PLIBERSEK—Is this another world first?

Mr Stuckey—No, it is not. It is a world first for an archives. We are a member of the international open office information systems group, and so we are sharing all this information. But I think from the perspective of a national archives it is. The national archives in Washington, for instance, has gone into partnership with the San Diego Supercomputer Centre to design something substantially more expensive. I did not have $US30 million to spend on this.

Ms PLIBERSEK—We have lots of records that deal with sensitive constituent information in our own offices. Do you have any suggestions for electorate offices about how we should store our sensitive information and preserve it for the future? What document could you guide us members of parliament to?

Mr Stuckey—We give pretty broad-ranging advice to members of parliament already through the parliamentary liaison group in the Department of Finance and Administration. The best thing for you to do is to backup and then backup to new versions. Generally, things are forward compatible, so Microsoft 2008 will pick up Microsoft 2006 but Microsoft 2006 will not read Microsoft 2008. You need to make to sure you keep up with the latest versions of the software.

Ms PLIBERSEK—Thanks.

Senator LUNDY—In your submission, you state that you have no power to require Commonwealth agencies to comply. Given that you are obviously working on and developing standards, do you think there is a place for legislation and the mandatory requirement of standards in this area?

Mr Stuckey—Yes.

Senator LUNDY—Thank you. I am familiar with the National Library's PANDORA system for web site storage. What are your views of PANDORA, and how does that fit into your vision for the accurate and perpetual storage of electronic information?

Mr Stuckey—We are cooperating with the library on the development of PANDORA. This starts to move towards that really interesting area of what is an electronic publication and what is an electronic record. It used to be quite simple when web sites were purely electronic publications telling people about who you were. Now, for example, the Centrelink web site actually transacts business between clients and Centrelink. Our advice to Centrelink is that, if they need information on their web site that is evidence of their interaction with the Australian people about rights and entitlements, it is important that in the Centrelink record keeping system they keep information about what is on the web site. If you claim against Centrelink because you go into the web site today, they change it tomorrow and the change is lost, it is your word against theirs. We advise agencies who are doing business via the Web, as opposed to just providing publication, to ensure that their record keeping system goes in and mines the transactions out of the Web. And that is part of our record keeping advice generally.

Senator LUNDY—I know that PANDORA has a very subjective and ad hoc approach to storing web sites, primarily because the National Library does not have the resources as an institution to do it in a more complete way. Is this something that, in your view, should be done

as a matter of course by each agency and department for their own web sites, presuming that the standards can be determined and, in effect, dictated to the agencies and departments?

Mr Stuckey—We provide advice to agencies that they need to keep a good record of their publications. That advice is media independent. Part of what people will be interested in about the way the Commonwealth operates is what sort of information the Commonwealth and its agencies provide to the public. Our disposal authorisation for all government agencies says: 'Keep a copy of your publications.' That does not help them a lot, though.

Senator LUNDY—No. But it comes back to my earlier question about whether mandatory standards or legislation are required. Obviously, with respect to web sites, you think a far stronger regulatory base is needed.

Mr Stuckey—Yes, I would agree.

Mr Cunningham—Can I just chip in on that. We have issued a policy statement and some fairly detailed guidelines for agencies on archiving their web based resources. We have also worked with the National Library and the National Office for the Information Economy to produce a joint brochure, which conveys a single message from our three agencies to the Commonwealth on what the responsibilities of Commonwealth agencies are and what some of the strategies that they can bring to bear on the issue are. Agencies might be dimly aware, thinking 'Well, there is PANDORA and the archives, but what does that mean for us?' and so forth. So we were quite keen to collaborate with those other organisations to produce a single suite of coherent advice to agencies. It is available as a leaflet, but it is also available on the web sites of our organisations.

Senator LUNDY—Can you provide a copy of that leaflet to the committee?

Mr Cunningham—Sure.

Senator LUNDY—Thank you. My next question relates to the Freedom of Information Act. That act permits access to Commonwealth records less than 30 years old in certain circumstances. How do the standards that you have established, and recommend be used, relate to the ability of a citizen to request information under FOI?

Mr Stuckey—FOI is also media independent. One of the things that we will argue to agencies to try to convince them to implement full and accurate record keeping is that they should be able to identify records in any format. Their attention is concentrated when they get discovery orders that include things such as their email systems. The requirement to identify either the broad sweep of a subject or individual email transactions, for instance, makes them realise that that is subject to FOI as well. Our advice would be that electronic records are records and are subject to FOI and, if you do it right, you will be able to identify them. You can go in and search your metadata.

Senator LUNDY—Finally, the whole issue of having some form of standard is obviously very important. Have you ever done an audit or a survey of how many agencies and departments are actually complying with your recommendations? Do you know what the level of acceptance of your advice is within agencies and departments?

Ms Dan—There were a number of surveys late last year—two that we conducted ourselves and one that the Australian Public Service Commission conducted in preparation for their State of the Service Report. The Public Service Commission asked at an agency level what agencies were doing in this area. We talked with them in the preparation for that survey and have also been able to access their results. That survey shows that people were saying that they were commencing along the path towards improving their record keeping. Many had not gone very far. The thing that came through that survey and also our own was that large agencies—portfolio departments—were tackling this; small agencies were not doing anything, I suspect this was largely because of resource concerns and also perhaps because of their skill and knowledge levels.

We conducted two surveys. One was of a random selection of individual public servants and it told us a lot about people's everyday practices. The thing that comes through from that is that many public servants feel that they are adequately keeping their information, because it is on their personal drive or it is on the network in a shared folder. But our evidence also shows that those things are not actually being managed within the agency; they are storage systems but they are not being managed. The second survey was of agencies—what they were doing in particular areas, which of our standards they had picked up and started to use, what the gaps were and what they would like us to be issuing them advice about. In that area, again, large agencies were doing more and small agencies were not. Most of the agencies that were doing something were starting to use the DIRKS manual but had not addressed some of the other areas—for example, they may not have looked at the record keeping metadata.

Senator LUNDY—In your work providing advice to agencies and departments have you ever found that the existence of a major IT contractor or subcontractor in some way presented a barrier to what you are trying to achieve, in the sense that they may have their own system that they have put forward as part of their value proposition to the agency or department? Conversely, what level of cooperation is there? I do not know if you are in a position to make any observations but do you know whether your involvement has evoked a need for contract negotiations and variation of contracts with IT service providers?

Ms Dan—I cannot think of a particular example where that has happened. Generally, our line is to talk with an agency about the importance of being clear on what their record keeping and information needs are at the commencement of negotiation and to make sure that that is documented in the contract. It is very much about advising them on what they need to have in place before they start that negotiation, to make sure there is a satisfactory outcome.

Mr Stuckey—Also, we deal independently with the contractors. For instance, when we were developing our standards we brought into the discussion groups the major IT developers and major IT vendors, the software people. Similarly, we deal independently, as the Commonwealth experts in this area, with the major contractors even before they start to contract to an agency. Once we are dealing with an agency, we deal with the agency.

Senator LUNDY—I would like to congratulate you on what you have been able to achieve in the development of standards, and I take this opportunity to acknowledge the role you have played in providing global leadership on several of these issues. You have done the Australian Public Service proud.

Mr Stuckey—Thank you.

Senator HUMPHRIES—You mentioned that there are jurisdictions that have adopted a strategic framework for information management and you cite a few of those. Which would you regard as the best practice model around the world at the moment for that sort of framework? You mentioned Canada and the UK, for example.

Ms Dan—I was going to say Canada.

Mr Stuckey—I think Canada.

Senator HUMPHRIES—When did it put its model in place?

Mr Stuckey—I cannot recall, but it was post 2000. We have dealt with the Canadians on international committees since the early nineties. A lot of the stuff we have done with the UK and the US has marched in step. There was a very strong push in Ottawa, from the nineties, to have a whole-of-government approach to information management. They mandated chief information officers, for example, in the early nineties and that put them well ahead of anybody else.

CHAIRMAN—We have a submission from the government of Victoria that describes the Victorian electronic records strategy, which I understand uses Adobe PDF.

Mr Stuckey—Yes.

CHAIRMAN—Have you looked at that and are you happy with it?

Mr Stuckey—We have indeed. Our initial nervousness was that it relied on Adobe, which is freeware but could be bought out by somebody. We found that the way that our two processes are developing is bringing them together, principally through the use of XML to wrap a document, so they are not incompatible.

CHAIRMAN—My advice is that you have not applied for Gatekeeper accreditation or registration and/or FedLink connection. Could you tell us why?

Mr Stuckey—I do not think we have any data that would require public key encryption.

CHAIRMAN—I asked you about the document *Australian government use of information and communications technology* and you said that you liked it. I have just gone through it and I cannot find record keeping anywhere except under ‘content management policy’, where it mentions the word ‘storage’. Outside of that, I have not been able to find record keeping anywhere.

Mr Stuckey—I think there is a terminological issue here. We use the term ‘record keeping’ because we think it important to tell people that they need to keep a record because it is evidence. I think, however, the intent of the report is very much the same, saying to agencies that there is a requirement for them to capture the information. I am not concerned about people using the terms ‘information’ and ‘records’ interchangeably.

CHAIRMAN—Thank you very much. If we have further questions, you will not mind if we put them in writing?

Mr Stuckey—Certainly not. We would be happy to answer them.

CHAIRMAN—Thank you very much.

[11.55 p.m.]

McMILLAN, Professor John Denison, Commonwealth Ombudsman, Office of the Commonwealth Ombudsman

TAYLOR, Mr John R., Senior Assistant Ombudsman, Professional Standards and Administration, Office of the Commonwealth Ombudsman

CHAIRMAN—I now welcome representatives of the Commonwealth Ombudsman to today's hearing. Thank you for your submission, which we have published. Do you have a brief opening statement?

Prof. McMillan—Yes, I will make a brief opening statement.

CHAIRMAN—Can you make it very brief, please.

Prof. McMillan—Firstly, I will preface my opening statement by saying that this is presently my third week in the job and every activity and outing is a steep learning curve. I will primarily highlight a few points in our submission and then I might rely more on Mr Taylor to answer questions. Our experience arose in three ways. Firstly, we are an office with substantial electronic record holdings, and that is outlined in our submission along with some of the steps that have been taken to ensure the security, integrity, safety and so on of information that is highly sensitive and personal. Secondly, our major role is to investigate complaints of defective administration against government agencies, and in the process of doing so we often turn up instances of problems that arise with or relate to electronic record keeping. There are none specifically outlined in the submission. There is a reference in general terms in our submission to some of the problems that we encounter. I have identified in, say, the last annual report and one of our special reports illustrative problems of defective administration that have relationships—an overlap in one way or another—with electronic record keeping. In the interests of brevity I will perhaps refer those to the committee at a later stage.

Thirdly, I was going to make the general observation that, in our experience of 25 years in investigating complaints against government administration, there is the broader dimension to this issue: every activity in and with government, as we see it, has an information aspect to it, whether it is to do with the way in which decisions are explained or recorded or the way in which information is analysed. Generally speaking, we see that information is a dimension of all government activity. In a general sense that simply highlights the importance of the issues under investigation by the committee. In the interests of brevity, I will perhaps curtail my brief opening statement at that point.

CHAIRMAN—Thank you. In your submission, you said:

> In my view, it is important for government agencies to have an effective and timely means of auditing access to electronic holdings.

Can you tell us a bit more about that and who you think ought to do the auditing?

Prof. McMillan—I will call on Mr Taylor in the first instance to answer these questions and then I might supplement with some observations as well.

Mr Taylor—Increasingly, Commonwealth agencies are relying on the collection of electronic data as opposed to paper. The move to a paperless office is real in our dealings particularly with the major agencies that are responsible for collecting and disseminating information about the personal affairs of people, such as Centrelink, the Child Support Agency, the Taxation Office and so on.

When we look at complaints about inappropriate access or release of information or when we are just looking at a complaint that relates to the treatment of an individual, invariably we want to be able to find out what information is held by the agency and who has been able to access it. To be able to audit the access is critical, particularly if the complaint is of a sensitive nature, such as the improper release of information. You only have to look at the Ombudsman's reports over the last 25 years to find that accessing government information has been a theme throughout most of those years.

As to the question of who should be able to audit it, a variety of agencies would need to be able to audit the access to Commonwealth information, including the Federal Police, other law enforcement agencies like ASIO and, of course, the Commonwealth Ombudsman. It would be obvious to you that we oversight a broad range of Commonwealth agencies, including law enforcement agencies, the recently created Australian Crime Commission, the Federal Police, the Department of Defence, the Taxation Office and so on.

CHAIRMAN—Do you have the right to look at my records?

Mr Taylor—A member of parliament is not within the jurisdiction of the Commonwealth Ombudsman. But, if you were to complain to us about an agency holding records relating to you, that would be a different matter.

CHAIRMAN—That was not the question; the question was quite specific. You also said in your submission:

> The current system is generally capable of operating reasonably well, although the experience of the Ombudsman's office suggests that agencies do not always look to their electronic records when they should.

Can you expand on that?

Mr Taylor—There are two aspects that I would respond to in relation to that. Firstly, there is the general issue of dealing with a complaint about the way a government department has handled an individual's affairs. Traditionally, agencies will respond with the paper file or paper records without any problems, and we have procedures for that. They are not the only records that will be held in relation to an individual; emails and other electronic data are often not considered in the same context as paper records. There is also a broader implication on which the Ombudsman is an expert, and that is freedom of information. Where we, as the Ombudsman, have a role in oversighting freedom of information complaints, invariably the electronic record is not produced unless specifically asked for. I think that is not a deliberate state of affairs; some agencies still do not see electronic information in the same context as paper records.

CHAIRMAN—Your submission mentions a number of information security measures that focus on staff: a clean desk policy, staff to acquaint themselves with office policy and all of that stuff. How effective do you think the measures are? I notice that you have failed to talk about security clearances.

Mr Taylor—I think our procedures are, by and large, effective, but we are a small organisation which has quite a deal of internal oversighting and complaint handling. For example, I am responsible for professional standards within the organisation, so I am well aware of our need to have audit trails internally and proper practices within the office in terms of record management. In that regard, as a small agency, our procedures are effective. In relation to how that translates into the broader Australian Public Service, we have done a number of examples of reviews and own motion investigations over the past few years which suggest that it is not a perfect world but, on the other hand, when we draw our concern to the attention of agencies, they respond well. An example that comes to mind is a report that we did in 1995 on the accessing and improper releasing of information by the Australian Federal Police. That led to some substantial changes in the way they operate and access information and how staff can look at information.

CHAIRMAN—How big is your agency?

Mr Taylor—It has 82.4 staff Australia wide.

CHAIRMAN—That seems very precise.

Mr Taylor—I also manage corporate services.

CHAIRMAN—Do the staff all have some degree of security clearance, and are security clearances by level of access?

Mr Taylor—There are two answers to that. Firstly, not all staff hold security clearances in terms of national security. Only staff who have access to documents that require a specific level of security have security clearances. For example, members of our law enforcement team—which deals with the Australian Federal Police, the Australian Crime Commission, intercept audit functions and various other audit functions—all have appropriate levels of security clearance.

CHAIRMAN—Are you up to date with the security clearances?

Mr Taylor—The answer is no.

CHAIRMAN—How far behind are you?

Mr Taylor—As staff change, it is necessary to make assessments for new officers. At the moment, we have a number of applications that are being processed. It takes time. There is a substantial delay in getting security clearances. There is no question about being behind; if a staff member does not have the appropriate level of clearance, they do not have access to documents.

CHAIRMAN—Has that been cramping your style, so to speak?

Mr Taylor—It does create limitations from time to time.

Ms PLIBERSEK—That is what I wanted to ask. We have had other departments appear before us, in other contexts, where the security clearances have not been up to date but the staff have been acting in those positions anyway.

CHAIRMAN—In fact, we had an inquiry on that.

Mr Taylor—The other issue for us, of course, is that the Ombudsman is a statutory independent officer and his staff are bound by the secrecy provisions of the Ombudsman Act. By and large, the bulk of our work does not require specific security clearances.

CHAIRMAN—Okay. Fair enough.

Ms PLIBERSEK—You state in your submission that you have found that the needs of the Ombudsman's office are best met by a centralised computer system that is not accessible from outside the office. Can you tell us about that system and how you exchange information electronically with systems outside the office?

Mr Taylor—The only way we presently exchange information outside the office is by email, and we do not exchange classified information that way. We do not have a secure email system, and we are not a member of FedLink. We are currently upgrading our firewall so that we will comply with the standards that are necessary for FedLink. Traditionally, because the Ombudsman is an independent officer, we have avoided having close electronic relationships with other Commonwealth agencies. But, with the increased oversighting role in the law enforcement area, we are reassessing that and upgrading our firewall. Within the next two weeks, we will be able to meet the standards established by Defence.

Our database is centralised. As a small agency, having distributed databases in each capital city—for example, we have one officer in Darwin, three in Perth and seven in Brisbane—would be a major cost to us. It is cheaper and easier to manage it by centralising. But it also makes it easier to protect. Because we are co-located with a number of state ombudsmen, it would be much harder to maintain physical security if we had a decentralised database. But cost is one of the major factors.

Ms PLIBERSEK—I am not quite clear on this. You say you have a centralised database. How do you transfer information from your state offices to that centralised database?

Mr Taylor—Simply put, by a telephone line. We use the Internet to communicate, and, the further away, the smaller the tube is that we pass information down. But it is by Internet.

Ms PLIBERSEK—Do you encrypt that information?

Mr Taylor—It is a dial-up, dial-back facility, so it is not encrypted. For example, if Perth wishes to access the database in Canberra, it dials up on the Internet the Canberra site, which dials back and ensures that it is the correct office.

Senator LUNDY—So it is like a virtual private network?

Mr Taylor—Yes.

CHAIRMAN—Is that good enough?

Senator LUNDY—Yes.

Ms PLIBERSEK—But you do not transmit any very sensitive information using the Internet?

Mr Taylor—No. Mostly the sensitive information that you might consider, such as issues relating to national security, defence or police, relates to documents held by the agency. If it is sensitive, we may only view it at the agency. It is unlikely that we would hold particularly sensitive national security level material ourselves.

Ms PLIBERSEK—And if there was sensitive information, if you needed to transmit it you would make a hard copy and—

Mr Taylor—If it was very sensitive, we would transmit it by hand.

CHAIRMAN—By what?

Mr Taylor—By hand. We would have it delivered.

Ms PLIBERSEK—Door to door.

CHAIRMAN—I am a little concerned about this dial-up business. If I am a telecom- enabled technician—that is, I understand the system—and I go out and go to a local junction box and pull the bomb-like cover off, I should be able to tap into your phone line and find out exactly what you are sending back and forth. If, for instance, there is a major investigation at the National Crime Authority or the Federal Police and you have a complaint from me, I might be able to go find out what is going on.

Mr Taylor—No, you would not be able to, because information on law enforcement matters is only dealt with in our Canberra office. No staff member outside of that law enforcement team has access to that database except for members of the executive, who are all based in Canberra. There would be no transmission across our system that related to law enforcement complaints. That is why we have set it up in that way: to minimise risk.

Senator LUNDY—To go a little further on the use of a virtual private network for the Ombudsman's office to connect, can you explain the security features of that type of technology?

Mr Taylor—I am not an IT expert, although I manage our IT area. I can only explain it in layman's terms.

Senator LUNDY—That is very good.

Mr Taylor—We have a database maintained in our Canberra office. We also have an electronic email system which is a generic email system—a Microsoft system—that anyone can buy. Our database can only be accessed by dialling up, which is done electronically, by one of our staff in Canberra or by an authorised staff member in the state. Our database is partitioned, so the user only has access to certain levels within the database, subject to their work needs.

Senator LUNDY—Can you confirm for me that each user has their own either pin or access identification so you can monitor whoever is accessing the VPN at any time?

Mr Taylor—Yes. There are two levels of accountability within the system. Firstly, to log on you have your user ID and a password. That gains you access to the desktop, which provides your basic day to day Word and other facilities for office work. Then through that desktop you have to dial up the database, again using an access identity and a password which is changed on a regular basis. Both systems are fully auditable. It is a routine part of my responsibility to ensure that audits are done on a regular basis to see, firstly, who is accessing the database and for what reason and, secondly, to audit Internet use.

CHAIRMAN—Good grief!

Senator LUNDY—The FedLink model is a virtual private network and operates on a similar system.

Mr Taylor—We have had advice from the Defence Signals Directorate on this, because we believe it is time that we move to FedLink.

Senator LUNDY—You have anticipated my next question beautifully. What is your view of FedLink, since obviously the system you have with your own offices shares the attributes of that system? Is it an option for you now to become part of FedLink for your access to government agencies and departments?

Mr Taylor—Yes, particularly in the law enforcement arena. I think it has not been that important in the past. Because we are an independent organisation with an oversight responsibility, much of our work is done at our own pace. In terms of law enforcement there is an increased emphasis by government, and our role has increased in terms of the responsibilities we have been given, which really require us to have regular contact and access.

Senator LUNDY—I know the Ombudsman's office has done a lot of work on contractual liabilities, relationships and accountability, particularly with contractors used by the federal government. Have you encountered any cases where the contractual layer between the complainant and the Commonwealth has traversed security related issues or has, in your view, compromised security in some way? If you can respond now that is great, but I am also happy for you take that question on notice.

Mr Taylor—Contractual issues have been an ongoing interest for the Ombudsman's office for some time. Successive ombudsmen have commented on the need for the Ombudsman to have jurisdiction over government contractors. A very topical example is the contractor who provides detention centre facilities for the government. Fortunately, we have not had a dispute with that contractor, because the department of immigration have written into their contract the need for the agency, which is currently ACM, to agree to the Ombudsman having access to any

information and to cooperating with the Ombudsman. That is not always the case with some government contractors. Another example that we have commented on in the past is Job Network providers, contractors who are providing employment services for the government. That is a more problematic area for us, but none of it has raised the issue of security.

Senator LUNDY—I will put to you a scenario: if a client of the Job Network felt that their privacy—as opposed to security, but it relates to data protection and security about data—had been breached and that clearly was in the control of the contractor, from your perspective do you have the scope to investigate the business operations and workings of that contractor in pursuit of the complainant's inquiry?

Mr Taylor—We have argued, so far successfully, that we do have jurisdiction, but we do not have jurisdiction in law—that is, the Ombudsman Act does not specifically provide for contractors. There have been occasions when departments have resisted our arguments, but right and commonsense have prevailed and we have been given access. It is a problematic area for us and it has been the argument of successive ombudsmen that the Ombudsman Act should be broadened to include contractors.

Senator LUNDY—Notwithstanding some cooperation from the departments, have you ever confronted a barrier with private companies that were not prepared to succumb to the advice of the department to open up their doors?

Mr Taylor—We have not had any direct knock-backs, but we have had to be very persuasive at times with both the department and the provider. But we look to the department—

Senator LUNDY—But that could in fact occur under the current law.

Mr Taylor—It is a real risk in the long term as the government continues to outsource what have traditionally been government services.

Senator LUNDY—Are you able to reflect on the issue of access to information held by contractors with large IT outsourcing contracts, perhaps with data held, managed or controlled or with business processes within those organisations? Are there any cases that you can refer to?

Mr Taylor—I think it is important to recognise that where there is a contract for those sorts of services the contract has conditions in it that would meet the sorts of risks that you are identifying. If that sort of complaint were brought to us, that is the first thing I would suggest we look at.

Senator LUNDY—The contract?

Mr Taylor—The contract provides for the protection of the Commonwealth data.

CHAIRMAN—We have recommended on more than one occasion that the Commonwealth Auditor-General be given right of access to every contractor to the Commonwealth government or any of its agencies. There is a Commonwealth government guideline, out of Finance, which recommends that the contracts include provision for A-G access, but there are still some instances—as with Centrelink and the Department of Defence from time to time, who cite the

need for commercial-in-confidence—where we strike an absolutely solid brick wall. I assume that you are saying that the Commonwealth Ombudsman falls into the same category and that you would like the same sort of access that we have continued to recommend for the Auditor-General.

Mr Taylor—Yes, that is so. I think the issue of commercial-in-confidence is not so persuasive with us, in the same category as legal professional privilege, because we are looking at what actually happened and the lessons for the future. We are looking to improve public administration, not necessarily to find fault or blame.

Prof. McMillan—For us, there are really two aspects to it. One is our jurisdiction to investigate complaints and the other is the powers that we can exercise in the course of those investigations. The first issue is whether we should be able to investigate a complaint against a private sector contractor in addition to a complaint against a government agency. The second issue is, assuming even that we had powers only in respect of government agencies, whether our powers to access information could nevertheless be exercised more broadly. Under the Ombudsman Act, at present they could.

CHAIRMAN—I can think of an instance, a particular contract, and there is no sense in going into the details now, where there was a breakdown in what you would call evidentiary procedure and where clearly I, as a member of parliament, could have come to you or to your predecessor and said, 'I would like you to investigate this breakdown. It occurred within an agency that was responsible to a contractor'—it was not even the contractor—'and I can't get access to the records. I would like you to investigate this issue.' I suspect that, like the Auditor-General, you would not have been able to access it. It can happen.

Prof. McMillan—Yes. Again, without breaking into the dangerous territory of giving a concluded opinion on the scope of my powers, our clear defined power is to investigate complaints against government agencies, but we can nevertheless exercise our powers more broadly.

CHAIRMAN—It could have been a department official who withheld information that we were looking for and that we could only gain by going to the agency responsible to the contractor. Anyhow, you have not talked to us the way the Auditor-General does.

Senator HUMPHRIES—Are you saying that the problem of access to the records of contractors should be fixed with legislative change to the Ombudsman Act or are you saying that this could be dealt with through a requirement that the Commonwealth government build in to all the contracts that they have access by the Ombudsman or the Auditor-General or whoever?

Prof. McMillan—I am subject to correction on this, but my recollection of the scheme of the Ombudsman Act is that, even if we are only investigating a government agency, we can still exercise our powers of inspection and questioning more broadly than that. So we could be asking questions and asking to look at the records of those outside the government arena. There is always the issue that you are more likely to come up against a lack of cooperation and you are more likely to get involved in litigation and protracted disputes. Certainly it has been the history of the Ombudsman's office that they have shied away from those for purely practical, functional reasons.

Mr Taylor—One of the issues when you are dealing with contractors is often a limited understanding of the role of the Commonwealth Ombudsman. They may have never dealt with the Ombudsman in the past, so the initial hurdle is to explain that we are interested in them as contractors, because they are providing a service to government—a service that may have been provided by government in the past. We are interested in how and where the money is being spent. To my knowledge, and I have been with the Ombudsman for some years, I am not aware of any contractor who at the end of the day has refused to cooperate, but sometimes it has taken quite a deal of negotiation and persuasion, including legal advice from eminent people like Professor Pearce in support of our arguments.

Senator HUMPHRIES—Are you saying that this should be fixed through change in the legislation?

Mr Taylor—Previous ombudsmen have made that recommendation to government on several occasions. To bring contractors within the jurisdiction of the Ombudsman would put to rest what has been a vexing issue for some years.

Senator HUMPHRIES—You do not mention that in this submission, but I suppose this is on a slightly different topic.

Mr Taylor—Indeed. We were purely focusing on the topic of your review.

Senator HUMPHRIES—You obviously receive complaints electronically by email. Can people make anonymous complaints to you, and do you act upon them if they do?

Mr Taylor—Yes. We reasonably regularly receive anonymous complaints. Our act does not require that a complainant have a standing or a specific interest in the complaint. We are interested in the substance of the complaint rather than the complainant. Of course, the issue has to have some legs, some merit, before we will investigate. It is not uncommon to get whistleblower complaints anonymously. There is a range of anonymity: they may wish to remain anonymous from the agency, they may wish to remain completely anonymous or they may wish to only contact us in particular ways. I will pick up on the beginning of your question—that is, electronic communication of complaints. That is a real growth area for us. Several years ago we were receiving complaints electronically in the tens. This financial year I expect it will be in excess of a thousand. We have had to very closely look at how we manage those complaints, put them on our database and make sure that our database maintains its integrity, and that is a big issue for us.

CHAIRMAN—To put things in perspective, even probably three years ago, I would be lucky if I got five emails a day. Now 100 is not unusual.

Mr Taylor—Yes, it is a sign of the times.

Senator HUMPHRIES—I would like to make a statement of congratulations to the Ombudsman on his appointment. I think you are the third Ombudsman to come from the ANU Law School. Well done. As a graduate of that school, I approve thoroughly.

Prof. McMillan—Thank you very much and thank you for the committee's indulgence of my relative silence on this outing.

CHAIRMAN—Thank you. I assume, if we have further questions, you will not mind if we put them in writing.

Proceedings suspended from 12.28 p.m. to 1.47 p.m.

DACEY, Mr Paul Edwin, Deputy Electoral Commissioner, Australian Electoral Commission

DAVIS, Ms Barbara Jane, First Assistant Commissioner, Business Support, Australian Electoral Commission

HUNTER, Mr Kenneth Robert, Assistant Commissioner, Information Technology, Australian Electoral Commission

MOYES, Mr Andrew David, Assistant Commissioner, Enrolment and Parliamentary Services, Australian Electoral Commission

NELSON, Ms Marie Patricia, Assistant Commissioner, Corporate Services, Australian Electoral Commission

POWER, Mr David Norman, Director, IT Business Services, Australian Electoral Commission

CHAIRMAN—I welcome witnesses from the Australian Electoral Commission. We have received your submission, which we have published. Mr Dacey, do you have a brief opening statement?

Mr Dacey—Yes, I do. I would like to thank the committee for inviting the AEC here today to assist the inquiry on this important topic. I do not think anybody here would argue that for over 100 years the AEC staff—or the staff of its predecessor organisations—have been protecting the integrity and confidentiality of the electoral process and the privacy of electors. This protection extends into the electronic means that we now use to carry out our business. Over recent times, the AEC has been subject to ANAO audits of the security of AEC systems and information. These include the audits into the integrity of the electoral roll and Internet security within Commonwealth government agencies. Both audits concluded that the AEC was effective in its security of electronic data and made a number of recommendations for further improvement. The recommendations have either been implemented already or their implementation is nearing completion.

The AEC also conducts regular reviews and analysis of IT security. Late last year a threat and risk analysis of our classification systems produced several recommendations for consideration, and just completed is a thorough gap-analysis of the *Protective Security Manual* requirements. In terms of current legislative guidance and framework, the principles applied by the AEC, as they relate to the security of our electronic material, are vested in two areas: the Commonwealth Electoral Act and the *Protective Security Manual*. Under section 91 of the electoral act, the AEC is required to provide roll information in electronic format to various bodies, including state governments, senators, members and political parties. The act also allows for the AEC to provide roll information to other Commonwealth agencies for law enforcement and revenue protection purposes and to approved medical researchers.

Whilst the AEC has no physical control of this information once it leaves the commission, section 91B of the Commonwealth Electoral Act provides for substantial penalties for its

unauthorised use. The AEC advises the recipients of this information of these penalties and of the requirement to protect the information. I would point out that the AEC has provided a significant submission on this issue to the current inquiry by the Joint Standing Committee on Electoral Matters into the 2001 federal election. Our submission, 147D, talks about a review of sections 89 to 92 of the Commonwealth Electoral Act. I invite the JCPAA to review this submission—and those recommendations relating to the privacy of the electoral roll—as it relates directly to this inquiry.

CHAIRMAN—Thank you. The submission of the Office of the Federal Privacy Commissioner mentioned an incident in 2000 where the AEC disclosed electoral data to the Australian Taxation Office for the purpose of a mail-out to support implementation of a new tax system. The Federal Privacy Commissioner concluded that there was no legal basis for the disclosure. Could you tell us about that?

Mr Dacey—We did not get to the point of disclosing the information. We were in the process of preparing for that disclosure and we had legal advice which supported our disclosure. However, we subsequently sought additional legal advice and withdrew that offer to the Australian Taxation Office. In fact, the legislation has since been amended to clarify the situation.

CHAIRMAN—Have you had any other major incident of an inappropriate disclosure of information?

Mr Dacey—No, we have not—not in terms of major incidents.

CHAIRMAN—My understanding is that you have a contract with CSC for the provision of information technology infrastructure. Can you tell us what sort of interaction you have with them?

Mr Hunter—We have quite a lot of interaction with CSC on all aspects of IT, particularly IT security. The contract requires that the CSC environment, as it pertains to the cluster and, in turn, the AEC, has to be DSD accredited. DSD have accredited that environment and they review that environment. In terms of security, every month we have a meeting with the CSC executive at a formal level—that is, at the cluster management committee level, executive level—where CSC presents quite a detailed security report. We also have working level meetings where our IT security people talk to CSC's IT security people to discuss any particular issues in detail. Of course, they immediately report any incidents that occur. There are very few incidents that have occurred.

CHAIRMAN—Do any of the organisation's employees have security clearance at any level?

Mr Hunter—Our organisation or the CSC?

CHAIRMAN—Your organisation.

Mr Hunter—Yes. We have security cleared executives at the moment, and that will be extended to other people as well.

CHAIRMAN—So you only have one person who is security cleared at any given level?

Mr Hunter—No.

CHAIRMAN—I am sorry, I did not hear you. You are not speaking very loudly.

Mr Hunter—We do have our senior executive security cleared. We are currently going through the process of also clearing people down the chain, so to speak.

CHAIRMAN—What sort of a backlog do you have on getting security clearance for your personnel?

Mr Hunter—Perhaps Ms Nelson can answer that.

Ms Nelson—At the moment we are waiting for two more people within the executive to have their clearance papers finalised. As Mr Hunter was saying, we will then move down the organisation and look at who else should be cleared, relative to the information they handle. We are at the stage of looking at that, so we do not have any backlog at this point.

CHAIRMAN—How about the contractor?

Mr Hunter—The contractor is required to have all of its staff who are working on the cluster environment security cleared, and I understand that that is the case.

CHAIRMAN—You said in your submission that the AEC is currently transitioning its desktop and help desk services back in house from out of house provision by, I assume, CSC.

Mr Hunter—That is right.

CHAIRMAN—Can you tell us about that and why you decided to do it?

Mr Hunter—Yes. You may recall that the Humphry report into IT outsourcing recommended that agencies at the end of their contract review the arrangements they had under the IT outsourcing initiative and make their own decisions on which way they would go. That might include continuing with the existing contract, moving to other contracts or, in fact, moving stuff in house. The AEC did a review of the contract with CSC, which is being extended as of 30 June this year. We started assessing that environment about 18 months ago, and about 12 months ago we made a decision that our best interests would be served by having our desktop services brought back in house but maintaining the mainframe, the midrange and some of the data services with CSC. I can go into the reasons for that, if you like.

CHAIRMAN—Yes; why?

Mr Hunter—The main reason is flexibility. You can appreciate that the AEC, at election time, have enormous changes in their environment, particularly the desktop environment. We roll out additional offices, tally rooms and lots of projects. CSC were not particularly good, in our view, at handling our requirement at that time. They used to do it, but it was problematic for us to manage those relationships. So we decided that we could do this service in house better

than the vendor could do it. Currently, we are probably about halfway through the whole project. We have rolled out our desktops right across the country and we have rolled out our new servers. There is a lot more work to go on in the background, but essentially we are very happy with the way things are working now.

CHAIRMAN—Did you do a cost-benefit analysis before you made that decision?

Mr Hunter—Yes, we did. That was done quite extensively.

CHAIRMAN—I assume it said: 'Go ahead.'

Mr Hunter—It did say to go ahead. There were not significant savings in terms of dollars; it was mainly a flexibility argument.

CHAIRMAN—I understand that you are not connected to FedLink and you are not Gatekeeper certified for either registration or accreditation. Can you tell us why?

Mr Hunter—We are not connected to FedLink yet, because we are part of the cluster which is currently going through the process of being connected. CSC provides our external gateway to the Internet, and that is the point where you bring in FedLink. FedLink will be available to all members of the cluster once it is installed.

CHAIRMAN—What is this cluster?

Mr Hunter—Cluster 3 was the first of the IT outsourcing initiatives, the first cluster or group of agencies to come together. It comprises Immigration, the AEC, parts of the electoral office network—your own network—Australian Government Analytical Laboratories, the national mapping agency and IP Australia. Those agencies got together about five years ago, put out one tender for all IT services and outsourced to CSC.

CHAIRMAN—Do you have any interaction with other government departments or instrumentalities?

Mr Hunter—We have some interaction, but probably not as much as a lot of other agencies do. We certainly have interactions with the department of finance and other members of the cluster.

Ms Davis—Perhaps, Mr Chairman, you could explain what you meant by interaction. We obviously interact with a lot of other government instrumentalities by way of our shared roll arrangements. Is that, specifically, the purpose of your question?

CHAIRMAN—What shared roll?

Mr Dacey—The electoral roll. We certainly have arrangements in place with state electoral authorities. We maintain the roll on a joint basis for the states, and we also have arrangements in place with some other Commonwealth agencies where we receive data from them so we can update the roll.

CHAIRMAN—You receive data from me, too, but that does not mean that any privacy or security information is involved. Is your interaction with those online?

Mr Dacey—No, it is not—but Immigration is sort of online.

Mr Moyes—Yes. We have access to Immigration's database for the purpose of checking people who are born outside of Australia to determine whether they are in fact eligible to be on the roll. Other than that, the interaction we have is not online. We do receive information from them, which might be in the form of a tape or a disk, and we then run that information against our database, but it is not online as such.

Ms PLIBERSEK—Would you receive information about deaths that way?

Mr Dacey—Yes, we do. That is not online but it is electronic. There is now a national fact of death file. It used to be that we received information from each of the states because each state was responsible. But there is now a national fact of death file, which we receive on a regular basis, and we match that against the electoral roll.

Ms PLIBERSEK—What action are you taking to ensure the long-term integrity of your archival information, information that you are not using day to day anymore? Do you follow the Archives of Australia suggestions on how to store any electronic information?

Ms Nelson—We do follow the archival guidelines both for hard copy and, in the main, for soft copy.

Ms PLIBERSEK—Have you experienced a lot of difference in staff attitudes to electronic information as compared with paper copies of information? We had evidence this morning that people find it easier to keep and store properly hard copies of information.

Mr Hunter—Yes, I think that is right. I think all agencies are facing that issue; it is a discipline issue within agencies as they enter more and more into electronic business. That is something that we are acutely aware of, and we try to make sure that everything electronic is filed either in hard copy or in electronic copy. But, yes, I think it is an issue that all agencies are facing, and it is a discipline we all need.

Ms PLIBERSEK—Can a person update their electoral enrolment over the Internet?

Mr Dacey—No, they cannot. They can download the form, but because the act requires a signature they have to print off the form, sign it and post it or fax it in.

Ms Davis—In relation to the problem of storing electronic information, the AEC has commenced a number of what are colloquially known as 'knowledge management initiatives' to ensure that staff become more aware of the necessity to store electronic information, a la the email traffic that goes ahead. So there are some specific initiatives we are undertaking at the moment, and will continue over the next year or so, to try to address this problem. I think you would probably find that is relatively common across the federal agencies.

Ms PLIBERSEK—In 2001 you took part in the ANAO performance audit of Internet security within Commonwealth government agencies. The report was entitled Audit report No. 13: *Internet Security within Commonwealth government agencies: 2001-02*. Would you brief the committee on the outcome of that audit?

Mr Hunter—In general, that audit was undertaken in conjunction with DSD, and DSD looked at our Internet web services and indicated they were satisfactory, with some recommendations for improvement, which have been implemented.

Ms PLIBERSEK—Have you taken up those recommendations?

Mr Hunter—Yes, we have.

Ms PLIBERSEK—Can you tell us what they were?

Mr Hunter—Yes. A recommendation was that the AEC revise its security policy, which was outdated at the time, and that has been done. Another was that the AEC continue to require CSC to provide regular reports on security related incidents; we do that. In fact, we do that with more vigour now than in the past.

Ms PLIBERSEK—I hope you do not mind if I interrupt you as we go along, because I will forget if I do not. You have revised your security policy; did you make major changes to that?

Mr Hunter—The policy has pretty well completely changed and, in fact, is still in draft form because we are in the middle of this infrastructure change. Essentially, it had to change because of the infrastructure. The basis for it was not changed, but some of the detail of it was changing.

Ms PLIBERSEK—So the operational things like how your staff use the systems have changed but the underlying principles have not?

Mr Hunter—The underlying principles really are principles and they do not change at all. For instance, we are not outsourced now—we do not have to go to CSC to change passwords and things like that.

Ms PLIBERSEK—The next point you made was that CSC regularly update you on breaches of security.

Mr Hunter—Yes, they update us on security in general. There are very few breaches—in fact, I cannot recall one in the recent past—but every month they provide a very detailed report on security right across the cluster. Have you heard of sweeping attacks on firewalls and what have you?

Ms PLIBERSEK—Yes.

Mr Hunter—The report includes things like that. Those attacks go on all the time—every agency has those in a firewall. CSC provide us with complete lists of those attacks, as I guess you could call them, that are intercepted. They list the particular viruses, trojans and so on that

they have detected—it is an assurance thing, basically. We also have our working level meetings, where that sort of stuff is discussed in more detail.

Ms PLIBERSEK—And going back to the ANAO recommendations?

Mr Hunter—Another recommendation was that CSC provide AEC with current documentation on network diagrams. We received that. Another recommendation was that the AEC request CSC to improve logging standards—that is currently under way. Logging across all of our systems is currently being reviewed and improved. Another recommendation was that the AEC request that CSC conduct a review of database drivers on the Web and remove some of the non-used functions of these applications. That is a best practice principle—it is not really a risk.

DSD said that the AEC web site is well protected and well configured and that appropriate procedures have been applied to ensure risk minimisation and strong security and operating systems. They said the web content is static and considered low risk in any case. They said that generally AEC has a secure web site, and they recommended we have a closer working relationship between the AEC and CSC, which we now have.

Ms PLIBERSEK—Isn't it true that cluster 3 are not renewing the contract with CSC?

Mr Hunter—That is not correct. In fact, they have extended the contract with CSC. Some of the agencies have decided not to remain in the cluster and have decided to go their own way.

Ms PLIBERSEK—So some have opted out.

Mr Hunter—In our case, we have decided to stay with CSC for some services but not others. That is really an outcome of the Humphry recommendations.

Ms PLIBERSEK—Were there any other ANAO recommendations from that report?

Mr Hunter—That is all I have got listed here.

Ms PLIBERSEK—In October 2002 the Joint Standing Committee on Electoral Matters reported on the integrity of the electoral roll. Do want to tell us a little bit about what the Joint Standing Committee on Electoral Matters found in relation to the integrity of your data?

Mr Hunter—I will ask Mr Moyes to answer that one.

Mr Moyes—The committee was looking at the report the ANAO did in respect of the integrity of the roll. There are a number of recommendations that the committee made. The government has not responded to that report as yet. Most of the recommendations are related to areas where we could have some improvement in roll integrity, in respect of the administration of the roll, management issues and also analysis that we ought to undertake in respect of the program we call continuous roll update, which replaced the 'doorknock' check of the roll.

The recommendations of the joint standing committee are fairly much in line with the recommendations that the ANAO made, which the AEC agreed with. We are now in the process

of planning the implementation of those recommendations. There is an issue of funding because, in our estimate, implementing those recommendations would mean a substantial injection of funds for us to be able to do them in a reasonable period of time.

Senator LUNDY—You mentioned the CSC reports on security and attempts to hack into your system. Do they provide disaggregated data particularly relating to your computers or do they provide a more general report to all of their client agencies within cluster 3?

Mr Hunter—It is a general report for the cluster, as I understand it.

Mr Power—Yes, it is on the actual secure gateway, which is the only entry point into the AEC environment.

Senator LUNDY—You cannot ascertain from that who is trying to break into AEC data?

Mr Power—These instances are typically not quite as deliberate as that. They are quite random and indiscriminate.

Senator LUNDY—Is there any way you can get a picture of the interests that hackers might have in your data assets compared to those of others within the cluster?

Mr Power—That is a major attribute of what you do in a risk assessment process, which is what we have just undergone. We look at the worth of our data in a variety of environments and, from that, we put our contingencies in place for it. You could say that, yes, that is actually what you do—you establish the value of your data.

Mr Hunter—It is fair to say also that, in terms of the major bulk of our private data—which is the electoral roll, of course—just getting through the gateway will not get them very far at all. There are far more layers of security under that before someone can get into the roll.

Senator LUNDY—I am trying to ascertain the impact of the cluster arrangement in effectively managing the contract via committee, and its impact on security. Can you perhaps reflect more extensively on the recommendations of the Humphry review, given that it evoked security concerns? I am also aware, as I am sure you are, of the security concerns in relation to the cluster 3 contract outlined in the ANAO report into the IT outsourcing in the three contracts, and how those impacted on you as an agency. What subsequent activities took place following that original IT outsourcing report by the ANAO and then the Humphry review?

Mr Hunter—When we originally signed up with CSC, there were quite strict security requirements in the contract. It did take quite a while for CSC to come to the mark on that but, to be fair to them, we now have one of the most secure environments I have seen, certainly in terms of any outsourcing that I have seen with vendor supplied services. It is quite secure. I am quite comfortable with it at this stage. It does require us to keep the vendor on the ball, but it would also require us to keep on the ball if we had it in house. We have not created new problems; we have just changed the problems we used to have before.

Senator LUNDY—The Humphry review was more explicit. The ANAO report identified the facts as they had occurred, and the weaknesses, and the Humphry review raised the spectre of ongoing security concerns. Was there any specific response arising from that?

Mr Hunter—No, there was no specific response on security in terms of what the cluster did, because at that time we were getting very close to having CSC where we really needed them, in terms of security. It is correct when you say that it requires continual monitoring. It does, but then so do your in-house things. I am not saying this is a fault of outsourcing; it is just the way things are. If you let security slip, it will slip wherever it is.

Senator LUNDY—Do you feel that you still have strategic control of security and privacy issues as an agency?

Mr Hunter—I would have to say that we do. We would have to liaise with our outsourcers on all those issues, but it is not difficult to liaise. It costs us money at times, but we do have it, I would say.

Senator LUNDY—And what about response times? If, as an organisation, you identify an issue, are you able to get a response from your outsourcer in a timely fashion? Are they meeting their service level agreements in performance? I guess I am not asking a prescriptive contract question. I am really asking you in the environment of heightened security awareness and new issues as they emerge.

Mr Hunter—There are no security levels surrounding security per se. Any security issues are wrapped up in the total service level bundle. CSC meet most service levels. I am not sure that there has been any month that I can recall when they have met every single service level—there are many, many service levels in the contract, so that does not surprise me. They have improved over time in terms of the service credits that are payable, so that indicates they are getting better. I am sorry, I have lost track of where I am.

Senator LUNDY—I am just trying to get a general impression. You said that the AEC has not proceeded with CSC in some aspects of the contract. What are those aspects and what are your reasons?

Mr Hunter—We decided not to proceed with the desktop services. There is the server environment and the internal email system on the desktop PCs. The reason for that was mainly flexibility surrounding election time—I answered the question a little while ago.

Senator LUNDY—Sorry.

Mr Hunter—That is okay. You can appreciate the ramping up we have to do at election time. We felt we could do that better.

Senator LUNDY—You do not want to have to negotiate a variation in the contract every time.

Mr Hunter—It is not a variation so much, but you are negotiating projects each time something happens and it is time consuming.

Senator LUNDY—I am sorry. I did not realise that you covered that earlier.

CHAIRMAN—The Management Advisory Committee of the APS put out their report No. 2 late last year, *Australian government use of information and communication technology: a new governance and investment framework*. Are you familiar with the document?

Mr Hunter—Yes. Well, I have read the document, but am not entirely familiar right at this minute because it has been some time since I have read it.

CHAIRMAN—I have read it very recently. You are comfortable with the direction that that group—the advisory committee and the chief information officers of the various departments—has arrived at, with that strategic change in direction?

Mr Hunter—Yes, I am. In fact, it would help us out quite a lot if the agenda that they have put in place were to come about, particularly the introduction of what they call a trusted government-wide computing system, which I believe is one of their main agenda items. That would overcome a lot of the problems we have currently with the disparate systems around the various agencies.

CHAIRMAN—Over a long time with this committee it has been my observation that lots of new things that you bring in tend to overshoot. It is like the very little simple on/off controller in your house that takes the temperature up. You set the thermostat and it brings the temperature on. It overshoots then it undershoots and eventually gets to the right point. About the time it gets where you want it, you change your mind and decide to change the temperature. We did that with government purchasing. We devolved it so broadly that there was no centralised command or control anywhere and we have decided to bring it back again. That is what this document reads like to me. Thank you very much for your evidence today. If we have further questions, you will not mind if we put them in writing rather than ask all of you to come back again, will you?

Mr Hunter—That is fine.

[2.22 p.m.]

KENT, Mr Philip Gregory, Executive Manager, Knowledge and Information Management, Commonwealth Scientific and Industrial Research Organisation

MORRISON, Mr Alan Geoffrey, Executive Manager, Information Security, Commonwealth Scientific and Industrial Research Organisation

WYATT, Mr Anthony George, IT Security Adviser, Commonwealth Scientific and Industrial Research Organisation

CHAIRMAN—I welcome representatives of the Commonwealth Scientific and Industrial Research Organisation appearing at today's hearing. We have received your submission, which we have published. Do you wish to make a brief opening statement?

Mr Kent—Yes. CSIRO welcomes the opportunity to meet with you today. Our submission reflects our background as a large, complicated, diverse scientific organisation within the Commonwealth. The submission makes some general observations about how we as a government agency respond to the plethora of guidelines, advice et cetera that we work within. Also, the submission looks at some of the issues associated with the management and integrity of Commonwealth electronic information as we have seen it in our own circumstances.

In particular, our submission covers mostly areas to do with security with some comments about the public key infrastructure encryption and those sorts of areas. In the area of record keeping, we also give some input from our experience with the risk assessment and audit side of things. Also, being a science organisation, it was good to include an outcome of one of our scientific projects, which is working from the CSIRO Mathematical and Information Sciences. Some of our scientists are working with the Victorian government on the Victorian Electronic Records Strategy, and particularly that part of our submission deals with their experience in the digital signatures area. That is essentially an introduction from us on our submission today.

CHAIRMAN—Thank you for that. I must make the comment that, of all the submissions I have read so far—and I have not read all the submissions we have received—I think I am correct in saying that yours is probably the most critical of the Commonwealth framework. You were particularly critical of Gatekeeper and FedLink. Your submission said of the Gatekeeper guidelines that they must:

> ... conform to a useful and consistent standard, but it is also a prohibitively expensive exercise, with only the largest organisations able to compete. This seems to be a costly duplication exercise for the Commonwealth Government and not consistent with a whole of government approach which would facilitate the uptake of PKI services.

It continued:

> It could be more useful to see a Commonwealth Root Certificate Authority created ...

Could you talk to those points?

Mr Kent—Mr Morrison can answer those questions for you, but it is also interesting to note that, while the PKI area is obviously important for our relationships with the rest of government within Australia, as an organisation operating in an international environment, we have to look more broadly than just at that environment. So while the PKI has some benefits in a defined area, I guess our horizons are a bit broader.

Mr Morrison—I think that is the key area because of our business requirements. We deal mainly with collaborative partners who are not necessarily government, so we deal outside of that government arena. In looking at the whole PKI environment outside of the government arena, a lot of our commercial partners do not actually care all that much.

CHAIRMAN—Why worry about it then?

Mr Morrison—It is about an acceptable protection of our information. In a lot of cases it comes down to negotiation with our partners as to, say, the confidential integrity requirements that they have and what we can actually put in place that makes sense. We have looked at establishing PKI initiatives internally, but it is really about a risk assessment of how much you need. To do this, we generally thought that it might be better to have a whole-of-government PKI infrastructure. We can certainly understand the tack that NOIE et cetera have taken in developing national industries, but, from an operational perspective, it can be a little onerous.

CHAIRMAN—I think we understood today—somebody correct me if I am wrong—that the United States and Canada are increasingly picking up Gatekeeper and implementing it in the public sector; I am not talking about the private sector. So why would we want to go backwards?

Mr Morrison—I suppose we are generally talking about the private sector. A lot of our international arrangements and even our collaborative arrangements in Australia are with private companies.

CHAIRMAN—I understand that, but I do not know why that would preclude the rest of the Commonwealth agencies from proceeding with that sort of encryption environment or enabler.

Mr Morrison—For the rest of the Commonwealth agencies, it is probably perfectly acceptable.

CHAIRMAN—I gathered from your submission that you thought it was all wrong.

Mr Morrison—No, definitely not. We were just looking at our business and the people we deal with.

CHAIRMAN—In terms of FedLink, which is a government agency to government agency intranet, your submission said:

Unfortunately, because of the wide-area bandwidth requirements (currently up to 10Gb), CSIRO is not able to use these services. CSIRO has a greater need for encryption with its national and international collaborators and it can be restrictive and difficult for CSIRO's customers to understand the need to use products endorsed on the Defence Signals Directorate Evaluated Product List.

If you are only talking about dealing with your client base—those who fund you, those you do collaborative research with or whatever—why do you need to worry about communication with other government departments?

Mr Morrison—It is more about the fact that, if this were mandated as a whole-of-government requirement, it would possibly become quite difficult for us to deal with external third parties. With the FedLink requirements, our wide area bandwidth for our research far outstrips what you can do with FedLink. Operationally, it is just really hard to make this thing work.

CHAIRMAN—I understand your differences and the needs you have for research, and I know that you operate, many times, in a real-time environment. I have also hung around your mainframe, located in the Bureau of Meteorology facility in Melbourne. So I am not unfamiliar with the issues, and at one point I fought for you too. But that is not the issue. We are talking about information technology security. Are you familiar with the document put out last October by the Management Advisory Committee of the APS called *Australian government use of information and communications technology: a new governance and investment framework*?

Mr Morrison—No, I am not.

CHAIRMAN—I recommend that to you. It talks about increasing levels of integrated architecture for a Commonwealth approach to IT issues, up to and including the role of the chief information officer. It is not up to me to give you advice, but it seems to me, if you are concerned about these issues with your customers and your clients—those for whom you do research and those, in addition to that, help to fund you and perhaps collaborate with you—that those issues are outside of the general sphere of the Commonwealth need for security and integrity of data. You are acting more like a private organisation which happens to be government funded, I think. Why don't you coordinate with that management committee and make your views known? I suggest this paper to you as well.

Mr Kent—Thanks.

Ms PLIBERSEK—Your submission calls for:

> ... a new 'Archives Act' which addresses the challenges of managing pervasive electronic information resources and records.

Do you really believe that the current act is inadequate?

Mr Kent—It is certainly not unworkable and, obviously, we have a very close and a very good relationship with the National Archives. That was not the intention of our comment. It is just that there has been some talk for some time about new archives legislation. It has been slow in coming, and we took this opportunity to encourage the Commonwealth to speed up that process.

Ms PLIBERSEK—What would you like to see in that new legislation?

Mr Kent—We have also noted in our comments—and I noticed it in the evidence of the previous witnesses—that the issue of electronic information and records is a big one. It is not

easy, and I think the National Archives have done good work in addressing this and giving us advice and direction. There has been lots of work done in the whole area of electronic record keeping, in particular on moving forward into archiving for the future, and Australia is recognised elsewhere in the world for having made some good inroads in that. But it would be a good opportunity to really push forward that electronic record keeping side with the new act.

Ms PLIBERSEK—Are there any specific changes you would like to see?

Mr Kent—Not at the moment. Maybe I could take that question on notice. Unfortunately, my colleague who heads up that area was unable to come at the very last minute.

Ms PLIBERSEK—If your colleague has anything that they want to add in that area, we would be interested in reading it.

Mr Kent—Sure.

Ms PLIBERSEK—You mention that the National Archives strategies are sometimes quite theoretical and that you could do with a bit more practical advice. We put that to the Archives people, and they said that that was not an uncommon complaint but they were trying to do a better job at that. Can you tell us what you would need for that advice to be more useful to you? What sort of help do you feel that you need from the Archives office for you to manage your issues around storing electronic data for the long term?

Mr Kent—Some further advice on how things could be implemented practically in a whole-of-government type of approach, because I can see different approaches happening in different organisations.

Ms PLIBERSEK—Do they come out and visit you and help you with systems design and stuff if you ask them to?

Mr Kent—They do. We are fortunate that we have a crossover of staff that have worked for us that work for them. The DIRKS methodology that we have been through recently was quite an involved and bureaucratic process. We found it a bit onerous and difficult. We felt that we probably got through it a little more easily because we knew some people there who understood the research environment. But it was a long and bureaucratic process. I think if those sorts of things could be facilitated that would make life easier for us.

Senator LUNDY—In your submission you make reference to the information security risk management guidelines but also raise the spectre of changing technologies and the relevance of those guidelines to new types of communication technology. You use wireless technology as an example. Can you tell me whether those risk management guidelines anticipate technological change and development in relation to new ways of communicating?

Mr Kent—What is good about the guidelines is that they are reasonably general, so you do not have to be specific. There have also been problems in the past with legislation on copyright and things like that about getting too specific. One of the reasons we value some of those risk management structures as tools for us to work with in the organisation is that they are not necessarily technology specific.

Senator LUNDY—To use a pretty obvious example, I presume you use the 802.11b standard at least somewhere in your organisation in terms of a local area network or something. Are those guidelines still relevant in adapting your security policies to the very specific security needs when using that type of technology?

Mr Morrison—General risk management principles apply there. You are looking at threats and impacts. We have used that to come up with two specific areas. One is almost a generic area where we have conferences with invited speakers who need Internet connectivity and, in looking at that, we have assessed the risk and then put controls in place to manage that. For more explicit access, we are trying to follow at least industry practice or better practice to manage the risk and then look at secure remote access and encryption to help us out there for controls.

Senator LUNDY—Another one that crossed my mind is the use of microwave for high bandwidth connections and so forth. What are the particular security risks associated with that type of technology? I am using this as an opportunity to get a bit of background again. You can take that on notice if you like. As an organisation you are probably well placed to give the committee an insight into some of those wireless types of technology and the security issues that relate to them—not necessarily issues that you have experienced, but generally.

Mr Morrison—As a quick general comment, we are moving away from a lot of our microwave connections as we can get fibre to the appropriate site. That has as much to do with increased bandwidth on fibre and reliability of services as it does with specific security issues.

Senator LUNDY—In general, the security risk management guidelines have a number of standards, some of which you have already gone through with Ms Plibersek. Do you think there is a need generally for legislation in the area of IT security, given that such a huge proportion of what we are dealing with here is still, in effect, advisory?

Mr Morrison—That is a very interesting question. In looking at security, we have used not only the *Protective Security Manual*, ACSI 33 and all the government things but also Australian standard 17799. We have found that extremely useful. Where we have trouble—and it is probably very similar with Archives—is with what constitutes a guideline and what constitutes a standard.

Senator LUNDY—So it is the status of those—a plethora of information?

Mr Morrison—It is to do with the use of some of the words. Sometimes the word 'must' is used, sometimes 'shall' and 'should'. That can get very confusing and can also be a bit of a loophole for people. So tightening up on that, applying common standards, is certainly a good first place to go to. That at least raises the watermark to the same level.

Senator LUNDY—So you think it is important that there is greater clarity in the way that those guidelines, codes and standards are expressed?

Mr Morrison—Yes.

Senator LUNDY—Are you involved in any way in the review of the PSM?

Mr Morrison—One of my colleagues is, yes.

Senator LUNDY—Is that an area where you think the language can be tightened up, or do think it should be upgraded in status?

Mr Morrison—I believe, from our discussions, that the language is being tightened up. I think that a reaffirmation to government agencies of the importance of the PSM could also be a useful thing.

Senator LUNDY—Do you think it needs to assume formal regulatory status?

Mr Morrison—It sits in a fairly uncertain place at the moment.

Senator LUNDY—I think it has, but there are lots of bits that sit underneath it that do not have formal regulatory status. From my understanding, it evokes a whole series of guides and other bits and pieces that form part of it.

Mr Morrison—That is where some of the confusion is. The PSM is fairly clearly mandated from letters from ministers. With some of the ACSI 33's and 61's and NOIE guidelines on a whole pile of stuff, it is a little bit everywhere.

Senator LUNDY—DSD have a system of reporting incidents, attempted hacking or breaches of security in IT systems. Do you use ISIDRAS and report any incidents of that nature to DSD?

Mr Morrison—We do not, generally, no.

Senator LUNDY—Is there a reason for that?

Mr Morrison—It is possibly the frequency of what is being expected of the ISIDRAS system. A while ago, at one of the government security seminars, someone from DSD wanted to know about network scans. They said: 'Should we report every network scan or should we batch them up on the day? If we get five for the day, do you want a day's report?' That is fine, except that we might get 12 million in a week. It is about the level of noise you have to deal with in actually connecting to the Internet.

Senator LUNDY—Is there anywhere outside of the organisation to which you report that level of interest in your IT data?

Mr Morrison—Depending on what it is, we would certainly be talking to AusCERT. That is usually on a 'for information' basis. The organisation has the skill to deal with it, you know what needs to be done. They generally cannot provide any additional information that we did not already know.

CHAIRMAN—Do you talk to the Bureau of Meteorology about these sorts of issues?

Mr Morrison—Yes, we do.

CHAIRMAN—Are there similar sorts of issues confronting you that are of concern?

Mr Morrison—The specific issues for the Bureau of Meteorology are around the joint arrangements with the supercomputer in Melbourne and the interaction that CSIRO has with the Bureau of Meteorology—who can get to whatever and from where.

CHAIRMAN—They would not be these 'in general' types of IT security and privacy issues?

Mr Morrison—That would be really only if we were dealing with some architectural or network type changes—how they would affect that particular arrangement.

CHAIRMAN—When they move buildings, will the supercomputer stay jointly owned?

Mr Morrison—I cannot answer that.

Mr Kent—With the joint arrangements and changing needs for technology of CSIRO and the bureau, a review of supercomputering has just recently been conducted. I am not sure of the outcome of that in terms of whether the arrangement is going to continue or not.

CHAIRMAN—I read in the newspaper—you always learn things in the newspaper, don't you!—that they are moving.

Mr Kent—Yes, they are moving to the Docklands in Melbourne.

CHAIRMAN—If they move, the supercomputer moves or else you do not have a joint use, I would suggest, because it cannot stay there.

Mr Kent—Yes, that is right.

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

Mr Kent—We would welcome them.

CHAIRMAN—Thank you.

[2.48 p.m.]

CLEMENT, Mr Trevor, Assistant Secretary, National Security Hotline, Attorney-General's Department

FORD, Mr Peter, First Assistant Secretary, Information and Security Law Division, Attorney-General's Department

LeROY, Mr Peter, General Manager, Information and Knowledge Services Group, Attorney-General's Department

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

Mr Clement—I am Assistant Secretary, Policy and Services Branch, PSCC.

CHAIRMAN—Thank you very much. Do you have a very brief opening statement?

Mr Ford—I would like to take the opportunity to table a document from the Organisation for Economic Cooperation and Development, OECD, *OECD guidelines for the security of information systems and networks: towards a culture of security*. I do so as the person who chaired the committee which drafted these. They were completed and released in August last year. I will very briefly outline them. The central point about these principles is the notion of a culture of security and the importance of developing that kind of thinking in everyone, from the consumer to the manufacturer. They are based on the idea that, in today's society, there is a networked system of information holdings, and that is quite different from the environment in 1992, when the previous OECD security guidelines were developed. They are intended to apply at a very general level, supporting national policies and so on, so they are quite consistent with documents such as the PSM, the Commonwealth Protective Security Manual.

They basically consist of nine principles. Very briefly, the first three principles are awareness, responsibility and response. They are the basis of the whole thing. Then there are another two principles, ethics and democracy, which really deal with the social interactions and the importance of one person's neglect of security to others. The final four principles are the more technical and detailed principles dealing with risk assessment, security design and implementation, security management and reassessments so that there will be continual improvement in security. But underlying the whole thing is very much the risk management philosophy.

CHAIRMAN—Thank you. In your submission, when talking about adequacy of public policy, you said:

> Based on a self-assessment by agencies, the PSPC believes that while there is no evidence of indifference to protecting official and security classified information, there are signs that a substantial number of Commonwealth agencies lack commitment to structured processes and practices that help to provide optimum security of information.

Mr Ford—Mr Clement will answer that.

Mr Clement—That statement was based on self-assessments by government agencies in their responses to an annual security survey. It might be useful to give a bit of history so you understand why the survey was conducted in the first place. The PSM has been around for 20-plus years but only in September 2000 did it move from being a set of guidelines to being endorsed by cabinet as a set of minimum mandatory standards. With that move to a compulsory set of standards, there was a requirement for agencies, or the Commonwealth Protective Security Policy Committee, to conduct an annual survey of security across the Commonwealth. That had never been done before. So we developed a questionnaire measuring an agency's performance against the minimum standards in the PSM. The responses we received from that survey were the basis of that decision.

A fact that came out of the survey was that 11 per cent of agencies said they had no classified information at all—nothing. That includes security-in-confidence and staff-in-confidence information, so their understanding of what is classified and what is not is questionable. Twenty-five per cent of agencies do not have an ITSO, an information technology security officer. So, a quarter of the agencies do not have a designated officer responsible for information technology. A lot of other data came out of the survey, but with that sort of response the concern was that this environment, where agencies have to comply with the minimum standards, is quite new for some agencies. One of the main purposes of the survey was to establish a benchmark so that in subsequent years when we conduct the survey we can measure the general improvement of security across the Commonwealth.

CHAIRMAN—You are the policemen.

Mr Clement—No, we are the policy setters. We do not actually go out and test. ANAO is probably closer to having the policeman's role; it conducts assessments.

CHAIRMAN—If things go wrong—if there are security breaches and there is a need to do something about it—you are the judge, the jury and the cop, in a sense.

Mr Clement—Actually, the policy guidelines are such that the secretary or chief executive officer of the agency is where the buck stops. That is the officer responsible for security within that agency. The PSM sets the standard. The agency head does have the ability to step aside from those minimum standards and can waive them if they deem it necessary for the particular operating circumstances of that agency. So we do not go in and test an agency's compliance with the PSM other than through the questionnaire.

CHAIRMAN—But if there are breaches and they are brought to you, you are the one who decides whether to prosecute. Is that not right?

Mr Clement—We do not have that role.

Mr Ford—I think the point Mr Clement is making is that the fundamental responsibility lies with the agency head. The PSCC sets the policy, subject to the government's direction. While it can make surveys and recommendations to agencies, it cannot cut across what the agency head says will be done.

Mr Clement—That is exactly right. If there is a breach, where some classified document has been released either accidentally or through some other means, and that is identified by the

agency then they generally bring that to the attention of the police and it is pursued through normal agency-police liaison and, if necessary, criminal action.

CHAIRMAN—So you do not get involved?

Mr Clement—We do not have a role in that.

CHAIRMAN—My understanding is that public servants who are prosecuted for certain breaches of the security act may be subject to jail penalties if they are found guilty. I am not aware that that is true of contractors. I think that is what we heard this morning.

Mr Clement—There is a portion of the PSM that deals specifically with outsourcing and contracting. It is a new part that we introduced in 2000. It says to the agency, 'If you are going to outsource any function at all, you are responsible to make sure that that function is carried out under the minimum requirements of the PSM across the range'—the physical protection of whatever information the contractor is working on, the security clearance of the contracting staff and ensuring that their IT systems meet the minimum requirements. That is all the responsibility of the agency that chooses to outsource a function to a contractor. So in that context the agency head is still the officer responsible.

Mr Ford—Subject to checking, I think the legal situation is that contractors are subject to some requirements under the Crimes Act and perhaps the more recent amendments. My recollection is of an extended definition of 'Commonwealth officer' in the Crimes Act. There may be more than that.

CHAIRMAN—The CSIRO, who have just been here—I think you were here during most of their evidence—called for a review of the Archives Act. Do you have a view about that?

Mr Ford—No. I suppose I have never given it any thought. We do not have responsibility for it and I have just not thought about it. I did hear the views presented but do not really have anything I could add.

CHAIRMAN—The A-G is a member of the Management Advisory Committee. Do you have a chief information officer?

Mr Ford—Yes. It is Mr LeRoy.

CHAIRMAN—Then you are more than familiar with report No. 2?

Mr LeRoy—Yes.

CHAIRMAN—Do you agree with the recommendations and the general direction of that report?

Mr LeRoy—Yes, I do. I think it is a good document. It is a first step in the right direction, but it is early days yet. We need to take care, but I think the process will mature. At the moment there seems to be a lot of overlap, with working groups being assigned tasks that are happening elsewhere in government, but as time goes on that will sort itself out. It is a very commonsense

thing to do. For too long we have been working along our own paths without a view to what is happening across government. I would look for a lot of efficiencies and a lot of mutual support amongst CIOs. It is very good to know what is happening in other agencies.

CHAIRMAN—How large is Attorney-General's in terms of the number of personnel?

Mr Ford—We number about 600.

Mr LeRoy—It may be a bit more now, with EMA. I would say the number is around the high 600s.

CHAIRMAN—I note that you are certified for FedLink.

Mr LeRoy—Yes.

CHAIRMAN—Did you find that financially onerous?

Mr LeRoy—Not at all. I forget the exact figure of the cost to us, but it was negligible.

CHAIRMAN—You have no need for Gatekeeper?

Mr LeRoy—I am very grateful for the fact that, at the moment, none of my colleagues has come up with a good use for it. When they do, I will have to do something about it. Without speaking for them, we have not identified a business need. Our interaction with other agencies and with the public is such that we have not yet come up with a need for authentication of that type.

Mr Ford—Speaking as one of Mr LeRoy's colleagues, I think the reason may be that other divisional heads, like me, are typically responsible for areas of policy development, development of legislation and so on, and there does not seem to us to be the need, at this stage anyway, to go down that track.

Senator LUNDY—Turning generally to the issue of the PSM and the process of updating it and making it more relevant, you said that its status changed in September 2000. What was the reasoning at the time?

Mr Clement—Prior to September 2000, the PSM was a document that contained general guidelines on good practice. It was made available to agency heads with the recommendation that they consider adopting it across their agencies so that there was consistency across government. But it was only that: a set of guidelines. Some agencies adopted it and some did not, and there was inconsistency across agencies. One of the aftermaths of the Wispelaere case was that the Inspector-General of Intelligence and Security, Mr Blick, did an inquiry. A recommendation from that inquiry was that the PSM should be reviewed, which was already in hand, that it should go to government for endorsement at the earliest opportunity and that it should become the minimum standard, and a number of other recommendations were made that have subsequently been adopted.

That was a major driver for the PSM to change status. Cabinet endorsed the PSM on 14 September 2000, we published the manual and sales started, I think, in December 2000. At the time it was recognised as a living document. There are eight parts in the PSM and we are reviewing as many of those parts as we can and as circumstances change. We are well under way with three of the parts, and they are very close to being ready to go to the Attorney for sign-off. We hope to reprint the PSM with the three new parts and an update to the other five parts later this calendar year.

Senator LUNDY—Thank you. In relation to the ongoing review process, what have you put in place to engage agencies and departments? Have you been able to get some quality feedback from them on the challenges they face in the implementation?

Mr Clement—We certainly do. The PSM is the policy document of the Protective Security Policy Committee. My branch provides the secretariat support to that committee, and we are members of it. The PSPC is made up of a number of agencies. Half of them operate in an environment where they are dealing with a lot of national security classified information. The other half of the committee do not have national security classification information and mainly deal with normal official in-confidence information. That was deliberate in an effort to keep the PSPC balanced so that the PSM is written to the lowest common denominator rather than the highest. The agencies that deal with a lot of classified data—particularly the intelligence community—operate at a much higher level than the minimum standards in the PSM.

When we come to reviewing parts of the PSM we call for expressions of interest from across the PSPC membership for agencies that have a view which they wish to be considered in the rewrite. Once a working group is developed, they then consider other agencies which are not members of the PSPC but may have a view on a rewrite of that particular part. We seek their input. So it is quite a detailed exercise.

Senator LUNDY—But it basically means that agencies not involved in that committee need to self-identify and say, 'We have a view and we want to be involved.'

Mr Clement—We have quite a wide network to get that in. Another of my functions is to run the Agency Security Adviser program. We conduct seminars to which all agency security advisers across government are invited and we run the Security in Government Conference every year. Evolving issues, where we need to update the PSM or introduce new policy, are discussed broadly in those venues. We do not have a set program as to which parts of the PSM are next reviewed. We look and see where the latest developments are and if there are any perceived weaknesses in the current policy, and we move on the priority items first.

Senator LUNDY—Earlier today we heard some feedback that because the PSM also coexists with a number of other guidelines and standards that sit within it—or beneath it, if you like—it lacks some clarity in language, for example in the use of 'must', 'should' or 'shall'. Is that something you are specifically looking at at the moment in the review?

Mr Clement—We were quite deliberate when we put this PSM to cabinet—in fact, the Attorney-General tightened up some of the aspects of it. When you read through the manual, when something reads, 'This must be done', it is a minimum standard. The 'shoulds' or 'highly recommendeds' are guidelines; they are not mandatory but are good practice. We recommend

that agencies adopt them, although it is not deemed by cabinet, in its endorsement, that they must be done. But the 'musts' are musts.

Senator LUNDY—What about subsidiary documents and standards? Is there a table which identifies those documents that the PSM refers to with an allocated status?

Mr Clement—The PSM refers the reader, particularly in the information security area, to DSD ACSI 33, which is a technical specification for the protection of information. The PSM does not go into that area; it does not want to shoot across DSD in that respect.

Senator LUNDY—But it evokes that and that is also a mandatory standard.

Mr Clement—It does not say that agencies must comply with ACSI 33. It says that for information and communication security technology advice we refer you to DSD ACSI 33.

Senator LUNDY—But is that a mandatory standard in itself?

Mr Clement—I would have to check that about 33. Some of them may be like that or not; I do not know.

Senator LUNDY—That is the issue; that lack of clarity about the status of those subsidiary documents was raised. Another issue has been raised, which is that, notwithstanding the difficulties about being technologically specific in any regulations, obviously new challenges come about as new technologies are deployed. What system or strategy do you have in place to ensure that the PSM continues to reflect those developments and no loopholes are inadvertently created by the progress of technological change?

Mr Clement—We have the agency security forums that we conduct and the feedback we get from agencies that participate in the Security in Government Conference. We have a consultancy role, and agency security advisers and IT security advisers do contact my policy section on almost a daily basis. They take half-a-dozen or a dozen calls every couple of days from agencies with specific inquiries about issues they are dealing with or grappling with that they need policy advice on. It is through that interaction that we identify emerging issues that are of concern. We feed that into the PSPC for discussion, and that helps us to identify the next part of the PSM that should be reviewed for whatever reason.

Senator LUNDY—I could probably ask you the same question in relation to privacy and technological developments in privacy. Do you have a view on whether the recently amended Privacy Act adequately addresses the challenges brought about by new and emerging technologies?

Mr Ford—To revert to your question before, I think you asked about technology neutrality, if I understood you correctly. The way I would answer is—

Senator LUNDY—I know there is a constant tension between the two things. You do not want to be too specific; you just want to make sure that it is embraced.

Mr Ford—I would put it this way. I think there is a need for both. You do need technology neutral principles, and you also need specificity as new problems, such as spam, emerge. The principles themselves—both the information privacy principles and the NPPs—are based on the OECD ones. I think they are technology neutral, and that view was also taken by ministers at a ministerial conference in Ottawa in 1998. They decided deliberately not to review them as they were still valid. At the same time, the Attorney-General has said that the act will be reviewed when it has been in operation for two years, and we reach that point in December this year.

Senator LUNDY—Do you think the penalties applying to hackers and people who illegally exploit vulnerabilities in IT systems are harsh enough?

Mr Ford—They have recently been updated. The Cybercrime Act 2001 includes new computer offences, based on a review of the form of the offences and the penalties by the Model Criminal Code Officers Committee.

Senator LUNDY—So you think that has addressed that issue adequately?

Mr Ford—Yes. I think they were the penalties thought appropriate by parliament.

Senator LUNDY—The Australian National Audit Office has published many reports, some of which in whole or in part address the performance of agencies and departments in relation to IT security. Does A-G's have a role in ensuring that agencies comply with those recommendations? If not, can you give me an insight into how there is some follow-up to ensure that those recommendations—presuming they are agreed to by government, of course—are actually followed and that there is accountability there?

Mr Clement—With respect to the ANAO's protective security audit series, they certainly talk to us about what areas are of concern. We assist them in developing their program of issues and what aspects of protective security should best be included in their audit process. So we do influence that to a degree, and we certainly assist ANAO in their efforts. On the related issue, I mentioned earlier that an agency head has the ability to step aside from the minimum standards and waive them if necessary. The PSM says it is acceptable to waive a minimum standard, but the agency head must advise the Auditor-General and the Secretary to the Attorney-General's Department that he or she is waiving a minimum standard. Prior to September 2000, the agency head just said, 'I'm not going to do it,' and did not have to tell anyone that they did not do it. But now there is visibility of that decision and, if matters of protection of national security are being waived, the Secretary to the Attorney-General's Department advises the Director-General of ASIO that department X is not protecting national security classified material to the appropriate standard. That process of having to notify when a waiver is being granted has, I think, tightened up considerably the waivers that were being issued prior to September 2000.

Senator LUNDY—I think that answered my question in part. The chairman earlier referred to a document called *Australian government use of information and communications technology: a new governance and investment framework*. I noted from that that both NOIE and A-G's have coordinating roles in the scheme of things. I also acknowledge the role you have in the critical infrastructure protection plans and initiatives. Can you describe for me the demarcation, I guess, between A-G's and NOIE on issues relating to IT security and IT-related critical infrastructure protection?

Mr Ford—Yes. I will start with the critical infrastructure protection. There is a group that I chair which is called the information infrastructure protection group. It was formerly called the critical infrastructure protection group. The name was changed to avoid confusion on the broader issue of protecting aspects of the critical infrastructure from physical attack. Although it has that rather broad description, it is really focused on the national security agencies—Defence, ASIO, AFP, ACC and so on. We meet once a month and focus on issues that are relevant to that kind of agency. NOIE chairs a group, which we also participate in, called the e-security information group. All government agencies can be members of that and it certainly has the agencies which are very important but not involved in national security. It is really a position that we have reached, with government approval, over a period of years. We started out more broadly and have gradually narrowed down our focus within Attorney-General's, and NOIE has picked up those other roles.

Senator LUNDY—In terms of the coordination of the very broad security agenda, what is the peak interdepartmental committee?

Mr Ford—It is the e-security group, which NOIE chairs.

Senator LUNDY—Do you keep records or surveys of attempted breaches or incidents? I understand that there is DSD's reporting service, but do you also, as a department, collate that information to help inform your policy development? Let me ask that, hopefully, a little more effectively. Do you have access to the incident reporting data collected by ISIDRAS in DSD?

Mr Ford—No, we do not.

Senator LUNDY—Do you have access to any incident statistics within the Commonwealth Public Service relating to e-security?

Mr Ford—It is changing now and that is why I am hesitating. With the group that I chair, which I referred to before, we are setting up an arrangement with AusCERT, the Australian Computer Emergency Response Team in Queensland, to provide an incident warning system to the broader Internet community and to collect data on incidents and so on. We will have access to that, but at the moment it is in its embryonic stages.

Senator LUNDY—Is the government, in policy terms, committed to AusCERT's ongoing presence and success in the role that they are playing?

Mr Ford—We have entered into a contract with them and this is the service they are providing.

Senator LUNDY—As far as roles and responsibilities go, my impression—and correct me if I am wrong—is that Defence Signals Directorate has had quite a significant amount of autonomy in standards setting with some aspects of e-security, particularly aspects relating to encryption standards. Are you able to comment on A-G's involvement in that policy setting process and do you have any observations that you are able to share about how that process can be improved and how that decision making can be more accountable?

Mr Ford—DSD are obviously the experts in this area. I think the process of policy formulation has worked well. We have worked closely with them on encryption policy over the years.

Senator LUNDY—Does that mean you are involved in the formulation of policy or do they tell you what it is after they have decided?

Mr Ford—No, we are not involved in the technical side. We—or at least I—would have nothing to contribute to their expertise on that sort of thing, but, for example, we were closely involved in the development of the policy that government agencies, if they choose to use encryption, must only use encryption products approved by DSD.

Senator LUNDY—Are there any other examples that are relevant to this point?

Mr Ford—Yes, there are a couple of areas. One area where I have some responsibility is that of telecommunications interception and the issues of encryption that can arise in that context. DSD are always helpful in working through those policies. The Attorney-General has responsibility, of course, but DSD are very helpful to us. They were also, I am sure, consulted by and involved with other areas of the department in developing the cybercrime legislation. It is a fairly close and successful working relationship.

Senator LUNDY—I know that DSD is attempting to make itself more accessible in providing advice to agencies and departments. Do you have any observations about the relative success of its endeavours to date and where you hope that will go in the future?

Mr Ford—I think it is becoming more successful. I was here when the CSIRO witness was asked about whether breaches had been reported to ISIDRAS and so on. The old attitude might have been, 'You are required to report things to us; if you do not, you are in breach of something,' but these days we are really seeking cooperation amongst agencies to report incidents and so on. We are certainly doing that in the broader community, with the critical infrastructure arrangements. I think it also works for the public sector. There are obviously mandatory requirements—Mr Clement has referred to those in the PSM and there is a place for that—but the point I am trying to make is that it seems to me that some of these reporting arrangements often work better if the agency doing the reporting is not in fear of being pilloried for having made a mistake, and agencies can together work through problems and learn from them.

Senator LUNDY—I do not think there would be many agencies that would disagree with you, but it still begs the question of whether the incident reporting should become mandatory, regardless of the subsequent confidentiality or otherwise attached to those reports. Could you respond in the first instance about whether or not you think incident reporting should be mandatory in some form, either to yourselves or to somewhere like DSD, for two reasons—first, so that there is a record of that there and perhaps remedial action taken and, second, for policy development and using that to inform what needs to happen next.

Mr Ford—Yes, I think incident reporting should be mandatory. The question, though—in my mind anyway—is: if it is mandatory and it has not been done, what then? How do we improve the situation? That is really where I was coming from.

Mr Clement—I would add that the security survey we conduct every year as part of the PSPC's efforts does have a series of questions on IT security. I would have to check the questionnaire to be absolutely sure but my sense is that there are some questions specifically on reporting attempts to attack IT systems. So, in that sense, there is a reporting to us. We then incorporate that in the response that goes forward every year to government for consideration.

Mr Ford—One of the problems was highlighted by one of the previous witnesses when he said that they had such a vast number these days that, if we put mandatory requirements on agencies, we would have to be very careful about how we express that so it does not become impossible.

Senator LUNDY—How do you engage with the private sector, particularly companies that operate in the IT security space? There are a number that are engaged in various capacities with Commonwealth agencies and departments.

Mr Ford—Tomorrow there will be the meeting of the National Summit on Critical Infrastructure Protection, which is to be held in Melbourne. That really follows on from the business government task force, which met in March last year and led to a number of recommendations that are being pursued by the government. They will be further discussed tomorrow and taken forward from that point.

Senator LUNDY—This is the trusted information security network.

Mr Ford—That is correct. One of the recommendations of the business government task force was to build a learning network, as it was referred to, of trusted information systems.

Senator LUNDY—What are the stated outcomes? What are you hoping for from tomorrow's forum?

Mr Ford—Personally speaking, it would be important to get some developments in areas such as communications and public utilities that lead to real improvements in security. I could not be more specific, other than that we get some real, practical improvements. I think it is an area in which everyone is learning, and we are improving over time.

Senator LUNDY—Going back to the more specific IT security companies, is there an industry forum in which you engage directly with those private companies?

Mr Ford—There are different sectors. There is a unit in my division that has regular contact with particular sectors, visits them from time to time and gives talks and that sort of thing. The ones we would have a lot to do with would be, for example, the Internet Industry Association and groups like that.

Senator LUNDY—What about some of the larger companies, which may or may not be global companies but they certainly operate internationally and in the Australian space? Is there one that you are aware of that NOIE has so that I can refer my questions back to them?

Mr Ford—The only forum as such that we are involved in is the business government task force. Flowing from that are the sectoral areas, which involve banks, public utilities and so on.

Senator LUNDY—Finally, there has been a significant amount of security technology innovation, which I am very proud to say has been brought about by various innovative Australian companies.

Mr Ford—Yes.

Senator LUNDY—How are you able to engage with those who are innovating in this area; do they have an opportunity to feed into your policy development?

Mr Ford—We would engage with them through the sectoral arrangements, but I guess that is still being built really. We do not have a formal arrangement in that we can say we meet with these people regularly, but we are trying to build that up to encourage the industry sectors to build their own groups in which government can play a part but which are really industry sectors rather than industry-government ones.

Senator LUNDY—I will make an observation there. I have seen it happen before that the very large players in the sector are those who have the resources to engage in policy development. By virtue of that, the policy solutions or strategies tend to reflect the model of service that those companies can provide. My observation is that that narrows the view with which the government looks at the problem.

Mr Ford—I understand the point. It is a difficult one. We in government are limited by resources, and in the private sector they are also limited by resources. Going back a few years, when we had the first iteration of this it was through something called the consultative industry forum. We tried to bring everyone together, and those who could afford to come tended to be the bigger ones.

Senator LUNDY—It invariably comes down to the initiative being in your hands, I suspect.

CHAIRMAN—I will add that it has been my observation, over a long period of time, that it is only closed societies that have unlimited resources.

Senator LUNDY—Thank you. We will get back to you if we have any more questions.

CHAIRMAN—Is it the wish of the committee that the document entitled *Summaries of ANAO reports No. 9 of 2000-2001 and No. 14 of 2002-2003* be taken as evidence and included in the committee records as exhibit No. 6 and that the document entitled *OECD guidelines for the security of information systems and networks: towards a culture of security* be taken as evidence and included in the committee records as exhibit No. 7? There being no objection, it is so ordered.

Senator LUNDY—Before we conclude, Mr Ford, how would you rate Australia's progress on matters relating to e-security relative to that of other comparable Western economies?

Mr Ford—I think we are well in the front ranks. I keep in regular contact, as do a number of my colleagues in A-G's and other departments, with my counterparts in the United States, the United Kingdom, Canada and so on. While each has a slightly different approach in terms of agencies and so on, we all learn from one another. I think we are doing okay.

Senator LUNDY—Thank you for that.

CHAIRMAN—Thank you very much for coming and talking to us today. It has been very good. If we have any further questions, we will ask them in writing. I thank those who have appeared, observers, my colleagues, the secretariat and, as always and most importantly, Hansard.

Resolved (on motion by **Senator Lundy**):

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 3.32 p.m.