COMMONWEALTH OF AUSTRALIA

Proof Committee Hansard

JOINT COMMITTEE OF PUBLIC ACCOUNTS AND AUDIT

Reference: Management and integrity of electronic information in the Commonwealth

MONDAY, 2 JUNE 2003

CANBERRA

BY AUTHORITY OF THE PARLIAMENT

[PROOF COPY]

INTERNET

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

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

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

JOINT COMMITTEE OF PUBLIC ACCOUNTS AND AUDIT

Monday, 2 June 2003

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

Senators and members in attendance: Senator Lundy, Mr Charles, Ms Grierson, Mr Peter King and Ms Plibersek

Terms of reference for the inquiry:

To inquire into and report on:

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

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

In conducting its inquiry the Committee will consider:

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

WITNESSES

CAMPBELL, Ms Kathryn, First Assistant Secretary, Social Welfare Division, Department of Finance and Administration 243

FLAVEL, Mr Matthew James, Branch Manager, Budget Coordination, Department of Finance and Administration 243

JAMIESON, Federal Agent William, Director, Professional Standards, Australian Federal Police 216

LOUDON, Mr Mike, Branch Manager, Procurement, Department of Finance and Administration 243

NICHOLSON, Mr John, Branch Manager, Infrastructure Branch, Department of Finance and Administration 243

O'CONNELL, Ms Lyn, General Manager, IT Services Division, Health Insurance Commission 230

RICHARDS, Dr Brian, Chief Information Officer, Health Insurance Commission 230

RYLES, Mr John, Director, Information Technology, Australian Federal Police 216

STAUN, Mr Dominic, General Manager, Financial and e-Solutions Group, Department of Finance and Administration 243

STINZIANI, Mr Antony, Branch Manager, Strategy and Service Management Branch, Department of Finance and Administration 243

Committee commenced at 9.44 a.m.

CHAIRMAN—I declare open this hearing of the Joint Committee of Public Accounts and Audit. Taking evidence is provided for in the Public Accounts and Audit Committee Act 1951 for its inquiry into the management and integrity of electronic information in the Commonwealth. I welcome everybody here this morning to the committee's fourth public hearing for this inquiry. A further hearing will be held in Canberra on 16 June 2003. Today we will hear evidence from three public sector agencies: the Australian Federal Police, the Health Insurance Commission and the Department of Finance and Administration.

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

JAMIESON, Federal Agent William, Director, Professional Standards, Australian Federal Police

RYLES, Mr John, Director, Information Technology, Australian Federal Police

CHAIRMAN—I welcome representatives of the Australian Federal Police to today's hearing. We have received your submission, for which we thank you. Do you wish to say a few brief opening words, or will we ask you questions about your submission and what you do?

Federal Agent Jamieson—If I might, sir: I would like to say at the outset that the Australian Federal Police takes a holistic approach to information, security and integrity and adopts that from a whole-of-government perspective, adopting both the Commonwealth Protective Security Manual and the Australian Federal Police Protective Security Manual in, if you like, a cradle to grave approach in relation to all our members and employees of the service, in that we structure our integrity area, which I am the director of, to incorporate both the security vetting side and the integrity side.

CHAIRMAN—Thank you for that. I note from your submission to us that in 2001 you did an internal audit which sponsored a thorough risk assessment of your in-house IT security situation and addressed the main issues raised in your security manual, electronic security instructions and a whole raft of codes of practice. You reported on the risk assessment and said that your audit committee, known as the Security and Audit Team, are monitoring progress against recommendations made as a result of that assessment. Can you tell us where you are at?

Mr Ryles—From an IT perspective, one of the major recommendations that came out of the threat and risk assessment was that, from a documentation perspective, we were informal rather than formal. The audit committee recommended that we have a very detailed inventory of our systems and equipment. We in fact have employed the services of a contractor and we are about two-thirds of the way, or possibly even further, through that particular exercise. That has been reported to the Security and Audit Team, and it is basically a work in progress.

CHAIRMAN—How many more pages does that add?

Mr Ryles—Actually it is not pages. We are doing it electronically from the perspective of charts, diagrams. We are at the stage now where we can drill down through the database and know where particular pieces of equipment are on the floor of the computer centre. One area that the threat and risk assessment looked at was our connections to other organisations, so this helps from a disaster recovery and a business continuity perspective.

CHAIRMAN—Considering the role that you play, I would think there would be a good deal of overlap or transfer of information between you and the Australian Crime Commission.

Mr Ryles—Yes, we do. In fact, the AFP also provides IT services to the commission.

CHAIRMAN—What have you done to secure that link?

Mr Ryles—We have a large, complex communication system which is encrypted. It is rated at the highly protected level, and we use DSD endorsed commercial security equipment to secure those links.

CHAIRMAN—Do you ever test it?

Mr Ryles—From the perspective of?

CHAIRMAN—Somebody pretending to be a provocateur and trying to gain access.

Mr Ryles—Tiger testing—no, we do not.

CHAIRMAN—Why not? Are you frightened of what you might find out?

Mr Ryles—Certainly not, because they are internal links. We do not go outside our own network. As I said earlier, we provide the backbone services to the Crime Commission.

CHAIRMAN—But how are you sure that somebody cannot get through into the network?

Mr Ryles—Because our external connections go through the secure gateway environment that is provided by a company called 90East, and 90East is a DSD evaluated security system.

CHAIRMAN—Why is it you use that instead of Gatekeeper?

Mr Ryles—Because the secure gateway environment was originally provided by—let me think now; what was it called in those days?—Agriculture.

CHAIRMAN—Sorry?

Mr Ryles—It was provided by the department of agriculture.

CHAIRMAN—Agriculture?

Mr Ryles—Yes. I doubt whether I can remember the right acronym. It was sold off as part of the outsourcing initiatives. We have been resident inside that gateway since 1997.

Federal Agent Jamieson—You talked about the audit. That is part of our fraud control anticorruption plan. We are in the third part of the finalisation of that plan, and it started renewal this year. It is currently due for review of its milestone steps by the Security and Audit Team in the August meeting.

CHAIRMAN—Returning to the gateway issue, in your mind what are the advantages of your gateway protection versus Gatekeeper?

Mr Ryles—They are two different things. We are one of the few organisations that have an accredited highly protected domain within the secure gateway environment. That is, as I said,

evaluated by DSD, and the organisation that provides that as a commercial service is reaccredited on a yearly basis to the highly protected level.

CHAIRMAN—How is that different to Gatekeeper?

Mr Ryles—Gatekeeper is not accredited to highly protected.

CHAIRMAN—I do not think I realised that.

Ms GRIERSON—Evidence we have received suggests otherwise, doesn't it? The National Office of the Information Economy have given us evidence suggesting that you do not use a gatekeeper which is an accredited authentication service, that you do not use one that they recognise; is that correct?

Mr Ryles—I think they may be incorrect.

Ms GRIERSON—They also suggest you are not connected to Fedlink, which is used by other government agencies.

Mr Ryles—Fedlink is protected at only the protected level. It is not a highly protected communications system.

Ms GRIERSON—So are you saying that DSD are satisfied with your systems in place?

Mr Ryles—We are not the only government agency that use the secure gateway environment provided by 90East. The Australian Customs Service services are located there.

Ms GRIERSON—So this was an outsourced contract. How did that happen?

Mr Ryles—It was a flow-on. It used to be provided by a government agency.

Ms GRIERSON—When did that happen? When did you change that?

Mr Ryles—That would again be 1999-2000. It was facilitated through NOIE's predecessor.

Ms GRIERSON—What do you think are the most significant risks to Internet information that you deal with, and have you made any prosecutions under these provisions?

Federal Agent Jamieson—Are you talking about internally?

Ms GRIERSON—Yes; we will start with that.

Federal Agent Jamieson—We identified the risk in our fraud control and anticorruption plan and we take a holistic approach to it. So this starts with recruitment: every person joining the organisation has to undertake a security clearance. Those operational members who access our systems to highly protected are cleared to highly protected before they are recruited. There is also a requirement for ongoing training at recruit level as well as ongoing training throughout

their service. There is also the standard recognition of the Commonwealth Protective Security Manual for ongoing training and awareness. We also conduct a number of spot check audits through my portfolio in relation to handling classified material and sensitive information. In relation to your question on prosecutions, we have not had any criminal prosecutions in the last 12 months for members disclosing information.

Ms GRIERSON—Have you had to take disciplinary action against anyone in that area?

Federal Agent Jamieson—Yes, we have. There was an incident recently, which is the most recent. Bear in mind our, if you like, Internet policy on the use of electronic flow of data inside the organisation is quite strict. There is a small allowance for private use, as many government agencies do. The scenario was that a number of members were given information concerning speed camera sites. That matter was investigated fully and has been referred to the deputy commissioner for consideration of sanctions against those members. The deputy decided in this instance to extend those members' probation for an extra six months.

I need to explain our discipline process to you, which is slightly different to the Australian Public Service process. Although we have discipline regulations under the Australian Federal Police (Discipline) Regulations, we have not invoked disciplinary charges or referred cases to the Australian Federal Police Disciplinary Tribunal for over 4½ years. That is because we have moved to a managerial model where there is either retraining, education and behaviour modification or dismissal from the organisation. Under the Australian Federal Police Act the commissioner has employer powers and command powers. In this instance the commissioner has delegated to the deputy and he has exercised the powers. So these people will be redeployed in a certain way and will be under strict supervision. These instances are picked up by our IT security and audit measures that are in place.

Ms GRIERSON—So was that information obtained by accessing other people's information, or was it sent to someone?

Federal Agent Jamieson—There was an incident where a number of the speed camera operators were being threatened by members of the public, because the speed camera locations were published. A general broadcast was sent to police patrols to monitor and look out for these cameras in certain areas over a certain period. A number of officers sent that information to other people, advising them of their locations. Clearly the commissioner considered that a very serious matter, because it is dealt with as information they obtained during the course of their duties.

Ms GRIERSON—What are your information exchange protocols with agencies like Customs, AMSA and AQIS that you work with a lot?

Federal Agent Jamieson—It depends on the type of work we are doing. For example, at Customs we have people who access PROMIS, which is our operational system. The AFP has an AFP LAN, which is worldwide, which is rated highly protected, and PROMIS, which is our operational system. We allow access by Customs and other agencies we work with in joint operations. They go through our vetting process and then are offered the training and told about the considerations in the handling of material, and then they are given access to our operational systems.

Ms GRIERSON—So there are controlled levels of access?

Federal Agent Jamieson—Correct.

Ms GRIERSON—But there is exchange of information between all those departments?

Federal Agent Jamieson—That is correct. Of course, it is fully auditable. Clearly there is a tension between 'have to know' law enforcement knowledge and security, as the Webster report from the FBI indicated. We are not immune from that tension. We need to ensure there is security of information and it is used appropriately, but we also need to ensure that law enforcement agencies are aware of that information-intelligence so they can do their job properly and with safety. So there is a fine balance there.

Ms GRIERSON—What about instances of corruption of information, compromising information or collapsing systems? In those cases would you enforce any of those penalty regimes or prosecution regimes?

Federal Agent Jamieson—Are you talking internally again, or are you talking about attacks on Commonwealth systems?

Ms GRIERSON—Attacks on Commonwealth systems from anywhere.

Federal Agent Jamieson—Yes, we do. Yes, we use the Criminal Code provisions. We investigate that as requested -

Ms GRIERSON—Do you think they are current with modern practice and modern threats?

Federal Agent Jamieson—The legislation?

Ms GRIERSON—Yes, and the penalties.

Federal Agent Jamieson—No, I do not think so.

Ms GRIERSON—Do you think greater penalties would be a greater deterrence or do you think that is beside the point?

Mr Ryles—I think it depends where the attack actually happens, which will always be a very difficult thing from the point of view of a cyberattack.

Ms GRIERSON—So are incidents increasing?

Mr Ryles—It is difficult to say. I know people are claiming there is an increase. However, in general terms I think the view still is that the greater threat is still internal.

Ms GRIERSON—Do you think particular departments, besides those that have secure information, are more prone to it?

Federal Agent Jamieson—I think it is difficult for us to answer that question. I am not familiar with their security systems, their processes or how they approach security from an internal perspective.

Ms GRIERSON—I mean those referred to you to pursue. Besides national security type departments, what other departments seem to have higher incident levels?

Mr Ryles—That particular aspect is handled by the High Tech Crime Centre, which is separate to our two organisations.

Ms GRIERSON—You do not interact with them?

Mr Ryles—Yes, we do interact with them. We provide some basic services to them. However, high-tech crime is a separate activity.

CHAIRMAN—I did not understand about the speed cameras incident. How did the Australian Federal Police get involve with speed cameras?

Federal Agent Jamieson—In the ACT we provide community services under contract to the ACT government. It is our system; therefore, we need to maintain the integrity of the system.

CHAIRMAN—There is no question about maintaining integrity; that is clear. The problem I had was with why on earth you were involved with speed cameras, because I thought your charter was a bit different to that. In fact, I am confident of that. At an operational level, I assume agents and office personnel et cetera could not do their job if they could not use the Internet. Is that right?

Federal Agent Jamieson—Correct.

CHAIRMAN—Are you subject to the same sorts of external problems of worms, viruses, snakes and ladders and all that stuff?

Mr Ryles—Our connection to the Internet, as I mentioned previously, is facilitated through the secure gateway environment. They provide an outer barrier. They also provide a service of virus checking. We then run our own internal firewalls and our own internal systems. In fact we run virus checking software that is different to that run by the secure gateway environment. That is a belt-and-braces approach. We also run virus checking software on our LAN service, which again is different, and we have the facility to run it on our desktops. So we have a reasonably good series of onion skin layers of protection.

Having said that, you cannot protect everything. But we also have a process whereby we train our users so that they know what to do if they receive an email—because email is becoming the way in which a lot of these worms and what have you are being transmitted—and they do not know where it comes from or it exhibits certain characteristics about which we get notification from our various suppliers of virus checking software. The advice is: ‘Do not open it; report it to IT security and they will look at it.’ Having said that, I would suggest that we pick up most, if not all, of the attacks at the perimeter barriers.

CHAIRMAN—How many times in the past five years has your system been penetrated?

Mr Ryles—Penetrated and had something actually affect the systems? Not at all.

CHAIRMAN—Very good.

Mr Ryles—We have never had a denial of service from that perspective, nor have we lost data.

CHAIRMAN—What sorts of links do you use when you communicate with Coastwatch? I would have thought that would require an extremely high degree of security.

Mr Ryles—I am not sure that we do connect to Coastwatch directly. I think we do it through Customs.

CHAIRMAN—Do you?

Mr Ryles—I would have to check that. I cannot recall anything on our network diagrams direct to Coastwatch.

CHAIRMAN—You have a role with Coastwatch which extends beyond Customs. It deals with fisheries, the environment and almost anything that goes on out there that Coastwatch is dealing with—immigration, the lot. You must surely have overseas information sources that you tap into all the time that you use in advising Coastwatch of potential threats or otherwise, of what is going on out there, so that they can do a good job in providing that barrier.

Mr Ryles—We have no direct connections to overseas agencies. That information is directed to us normally through our network of overseas liaison officers, and we have highly protected connections to those officers.

CHAIRMAN—Are you familiar with the Management Advisory Committee's report entitled *Australian government use of information and communications technology: a new governance and investment framework*?

Mr Ryles—I am familiar with it; I would not say—

CHAIRMAN—It seems to me the general thrust of this report is setting up, if you will, a federation style control architecture to deal with all of the public sector and agencies that operate in or for the public sector—anybody who falls outside the CAC Act or FMA Act, in other words. To that extent, do you approve of that coordinated approach?

Mr Ryles—The AFP is a member of the security infrastructure committee being chaired by NOIE. We are also on the technical working parties.

CHAIRMAN—Is that working well?

Mr Ryles—I believe so. I believe they have almost finished their initial reports. I believe some areas will still have to be explored, especially with those agencies that also handle national security information.

Ms GRIERSON—If you have breaches, incidents, and you keep a record of your own incidents, do you then convey them to a central body?

Mr Ryles—There is a body. DSD have a system called ISIDRAS. I cannot remember what that acronym stands for.

Ms GRIERSON—So basically it is DSD?

Mr Ryles—DSD have established a central repository to collate those types of—

Ms GRIERSON—From all Commonwealth departments?

Mr Ryles—From all Commonwealth departments.

Ms GRIERSON—In a previous audit we looked at whether each Commonwealth department had updated its security checks on all its staff. Where are you at in terms of your security checks on all staff?

Federal Agent Jamieson—We have just finished doing an audit of all our clearances, and we are progressing down that path. I would say that we are probably three months out from completing that. In a report to the Attorney-General's Department we are on track in relation to our security clearances. Bear in mind that our processes are above that of the standard level of the Commonwealth Protective Security Manual.

Ms GRIERSON—So they are continuous?

Federal Agent Jamieson—Continuous. But since our basic level is 'highly protected' for sworn members there are added checks that are not put into the normal Commonwealth Protective Security Manual level. For example, we undertake face-to-face security interviews for all staff. Added to that layer, we also do unnominated referee interviews, mainly because we take the view in our organisation that, although IT provides a good coverage and security framework for us, we do not depend on it solely. The principle we adopt is that our biggest threat is people, so we educate and program in so that people understand the implications and ramifications of certain sorts of behaviours.

Senator LUNDY—Can I ask what might seem an unrelated question: how long have AFP officers called themselves 'agents'?

Federal Agent Jamieson—That has been since 1995, when the then commissioner, Mick Palmer, requested that change through the parliament. It is under the act. There is local nomenclature. In the ACT, for example, they still use the local titles of 'constable' and 'sergeant', but nationally it is 'federal agent'.

Senator LUNDY—The ISIDRAS is non-compulsory at the moment. I take it the AFP choose to provide the detail to DSD?

Mr Ryles—That is correct. It is non-compulsory. In many respects it follows a similar line to the AusCert process.

Senator LUNDY—Obviously you are a supporter of AusCert and participate in the AusCert process?

Mr Ryles—We have participated in AusCert, and some of the other agents or parts of the AFP that deal with computer forensics and high-tech crime are also involved with AusCert.

Senator LUNDY—In terms of the AFP's role in the security infrastructure working group as part of the NOIE e-security initiative, what other subgroups are you involved in as part of those whole-of-government gatherings?

Mr Ryles—Our information management area is involved, again with NOIE, with the various e-commerce working parties—government online. Our high-tech crime people are also involved, again I think with NOIE, with e-crime and e-security.

Senator LUNDY—Do you filter email for your employees?

Mr Ryles—In what way?

Senator LUNDY—Firstly, by using software to filter out spam email.

Mr Ryles—We have the capability to do so. However, we do not actually filter. We do quite a bit of content management from the point of view of finding out what is going in and out of the AFP. In fact, we log all the traffic in and out.

Senator LUNDY—Yes, I think most organisations do.

Mr Ryles—We also run some software that looks at images, but it is still relatively immature, unfortunately, in that it is looking for, in the main, groupings and skin tones. This is the sort of thing where, say, pornographic images may be attached to an email. It is still, as I say, immature and provides a lot of false positives, in that things have been stopped when in fact it has been someone sitting on a motorcycle or someone holding a baby. But we do have that capability.

Senator LUNDY—Monitoring of email is obviously part of an email policy.

Mr Ryles—Yes, it is.

Senator LUNDY—What is the security issue that you see linked to that monitoring program?

Mr Ryles—The threat?

Senator LUNDY—Yes.

Mr Ryles—I think in the main it is inappropriate use of email, and there is also the issue of denial-of-service attacks through viruses, spam, spoofing or something like that.

Federal Agent Jamieson—There is a strong policy under the commissioner's orders in relation to this, about behaviours and values. We do not go down a prescriptive path, but certainly if an employee misuses emails it is brought to my office's attention and we deal with it appropriately with an investigation, either a security investigation or an integrity investigation, depending on the nature of the material.

Senator LUNDY—It is proactive monitoring?

Federal Agent Jamieson—We have both a reactive and a proactive monitoring.

Senator LUNDY—Does the same sort of thing apply to use of the Internet and Web addresses?

Mr Ryles—Essentially it was agreed some years ago that free access would be allowed to the Internet because, again, it is difficult to prescribe what our members may or may not be interested in in pursuit of their operational requirements. So we do have a system of proactive and reactive logging and monitoring. We also have a fairly strict policy. When people are originally given their access rights, they sign an undertaking so that they understand what they should and should not be doing. We also reserve the right to stop mail, open mail, delete mail, record it, and a whole string of things such as that.

Federal Agent Jamieson—We also have an education program for members involved in that sort of activity, plus warnings on all the screens advising them of the Criminal Code breaches as well as the discipline breaches if they do behave outside the scope.

Senator LUNDY—But you do not filter the Internet, or the Web content?

Mr Ryles—The technologies are fairly simple but, again, because of the range of activities that our members are engaged in, it would be very difficult. Some people may have a reasonable excuse to visit a certain site.

Senator LUNDY—It might be part of an investigation.

Mr Ryles—Precisely.

Senator LUNDY—What are the AFP's IT outsourcing arrangements? Who are the major IT contractors?

Mr Ryles—We were part of the group 10 outsourcing initiative that was cancelled. We mainly insource, in that about a third of our IT staff are contractors. We obviously use the services of 90East, for example. That is outsourced.

Senator LUNDY—For FedLink?

Mr Ryles—We do not connect to FedLink, although we have the possibility of doing so through 90East.

Senator LUNDY—I was going to ask you about that.

CHAIRMAN—Why aren't you connected?

Mr Ryles—The people whom we do business with in the main are connected through FLAGNet, a federal law enforcement grid which is an old thing left over from the mainframe days which was translated into the secure gateway environment and which runs at 'highly protected' level, whereas FedLink runs at only 'protected' level. Having said that, we have recently been approached by AUSTRAC, who are looking at using FedLink for their basic connections. But that essentially is something to do with cost, I think.

Senator LUNDY—Apart from 90East, who are the significant contractors that you use for IT services?

Mr Ryles—Obviously we use a lot of service providers/carriers: Telstra, Optus, Vodafone. They are probably the major service providers.

Senator LUNDY—Are your software services and applications, for example, in house?

Mr Ryles—Application development is in house. We run our own midrange systems in house. We run our security services in house.

Senator LUNDY—Is that using a standard package of software or software you have developed yourself?

Mr Ryles—We are using standard packages. For example, we are in the process of moving from Visual Basic to .NET for developing our major operational application, an application called PROMIS.

Senator LUNDY—Called what?

Mr Ryles—PROMIS—Police Realtime Operational Management Information System.

Senator LUNDY—Very good. That is the best acronym I have heard for a long time.

Mr Ryles—There is a history to that, which I am not sure will add anything.

Senator LUNDY—I have a couple of questions in relation to that. To what extent has the AFP investigated the use of open source software? This committee has heard a wide range of views about the security attributes of different types of proprietary software and open source software.

Mr Ryles—At the moment, we are basically going to commercial software.

Senator LUNDY—Open source can be commercial.

Mr Ryles—Yes. We flirted with Linux, and indeed this is not to say that we would not go back to Linux in about three years time.

Senator LUNDY—I had in my mind that you have used or are using some type of open source software. Where would I have heard that? I might be incorrect, of course.

Mr Ryles—There may be some small application that I cannot bring to mind, but in the main it is things like UNIX, Oracle, Visual Basic, .NET, and the commercial language that goes along with SAP. We are now moving into Web services, but, again, that really comes back down to a bit of jargon and mainly .NET.

Senator LUNDY—Are you able to provide the committee with some observations about the AFP's decision to retain so much of their IT services in house, particularly in the context of whether that was a security consideration?

Mr Ryles—Partially. We also found that, by doing software development in house, we do it considerably faster.

Senator LUNDY—So it is as much an efficiency question?

Mr Ryles—It is efficiency, it is cost, it is security. We are able to control the code. We do our own testing.

Senator LUNDY—What about in terms of controlling code? One of the key themes of the report the chair mentioned is interoperability and the ability of systems to work together if required. How much does that ability or the use of non-proprietary software currently factor into your decision making?

Mr Ryles—It is proprietary software. It is just the programs that we write using those languages. We provide a copy of PROMIS to the Northern Territory Police, Fire and Emergency Services.

Senator LUNDY—Is that on a cost recovery basis, or do you actually make a quid out of it?

Mr Ryles—No; it is pass through costs, really. We also provide services to the Crime Commission. They also use PROMIS.

Senator LUNDY—So you have developed it in house?

Mr Ryles—We have developed it in house, and it is now being used by two other law enforcement agencies. In fact, with the Crime Commission we manage the environment.

Senator LUNDY—What does PROMIS do?

Federal Agent Jamieson—PROMIS is our operational management system where all our cases are recorded and evaluated, along with all the, if you like, running sheets, occurrences, statements, information reports. All that information and data are loaded onto the system. We have, as I mentioned earlier, a tension in law enforcement between security and sharing

information. It does not matter where an agent is, if they have access to the system they can see what is going on in any particular case at any particular time.

Ms GRIERSON—If I were being investigated for social security fraud or taxation fraud, would I be on that system?

Federal Agent Jamieson—If it has been referred to the AFP, yes.

Mr Ryles—If a case has been opened, there will be—

Ms GRIERSON—Who would have access to that?

Mr Ryles—It really does depend on what is happening. In most cases the information is restricted to the members of the investigation team. At some later stage there is a review, because the aim obviously is to reduce the islands of information.

Ms GRIERSON—So are you telling me not every person who is employed by the AFP could access it?

Mr Ryles—No, correct.

Ms GRIERSON—Only the ones who are working on that. How does that happen?

Federal Agent Jamieson—To clarify that point: if your name goes on the database and someone needs to know that you are on the system—for example, if we want a person of interest—it would be a ridiculous scenario if a law enforcement agent or anyone with that access clearance could not see the name and then why they are of interest. It is important to understand that. So it might not be just that team. It depends on their level of information, because we can layer it. For example, we might want the whole organisation who are operational to know about a certain individual but not the detail of what is there, so their name will come up.

Senator LUNDY—Is there an automatic process for crosschecking? If you have a name that has popped up in a few different contexts, does your system pick that up or do you rely on humans to go searching for coincidences?

Mr Ryles—There is a combination of that at the moment in that we do have some text retrieval tools, but we are looking at a greater level of automation. There are pros and cons, to be honest, about how that is done, because you still need that human element to determine that two John Smiths could be two different John Smiths.

Federal Agent Jamieson—That is verified through the normal identification procedures—fingerprints et cetera.

Senator LUNDY—Do you have a view on the merits or otherwise of legislating a minimum standard for the security requirements in that electronic environment? Again, at the moment it is all guidelines, recommendations; different agencies and departments choose for themselves effectively how hard they go.

Mr Ryles—I cannot see that there would be necessarily a problem there. There is a balance. You have security functionality and you have cost. There will always be that split. The AFP, wherever possible, chooses to implement the Australian communication security instructions which are issued by DSD. We look at the Australian standards, which essentially again almost mirror those same instructions from DSD. So wherever possible we try to meet those standards, and in fact go better than those standards.

Federal Agent Jamieson—The reason for that is, if we do not, the agency that owns the information is not likely to share it with us; and we would have the same view of another agency that does not have appropriate standards.

Senator LUNDY—So for any sort of data matching or sharing of information that you require, you demand certain standards of other agencies?

Mr Ryles—For the exchange of information, yes, we demand a minimum standard of security.

CHAIRMAN—Thank you very much for coming and thank you for being so cooperative in answering our questions. If we have further questions, you will not mind if we put them to you in writing to save asking you to come back again?

Federal Agent Jamieson—Not at all.

CHAIRMAN—That would be very good. Thank you very much.

[10.30 a.m.]

O'CONNELL, Ms Lyn, General Manager, IT Services Division, Health Insurance Commission

RICHARDS, Dr Brian, Chief Information Officer, Health Insurance Commission

CHAIRMAN—I welcome the representatives of the Health Insurance Commission to today's hearing. Thank you very much for coming today. I understand that you have not given us a submission, but we have taken some information off your web site. That is sneaky, isn't it.

Dr Richards—All part of the service.

CHAIRMAN—Do you wish to make a very brief opening statement, or can we start asking you questions?

Dr Richards—Just very briefly, HIC takes its information, privacy and security issues very seriously. We are subject to the secrecy provisions of both the National Health Act and the Health Insurance Act, as well as the provisions of the Privacy Act. We are certainly happy to answer any questions in relation to the way in which we manage personal information.

CHAIRMAN—In our initial round of public hearings we talked to representatives of the Department of Health and Ageing. In discussions with them the name of your agency came up so many times that we determined we had to talk to you. You seem to be such a major player in this area. I do know that in 2001 ANAO did a performance audit which included you. Can you tell us the outcome of that audit with respect to the HIC?

Ms O'Connell—Yes, certainly. Are you referring to the audit on IT in the HIC?

CHAIRMAN—Yes.

Ms O'Connell—Out of that there were six recommendations. I can briefly go through them if you wish, but of those six recommendations we agreed in our response to all of the recommendations from the ANAO. Of all of those six, we have fully implemented five of the recommendations and have one that is partially implemented and is just awaiting some final activity this coming financial year to complete it. Then that will see us having implemented all six of those recommendations fully.

CHAIRMAN—I have just been looking at your web site. You are responsible for administering a heck of a lot of programs, from Medicare to payments and claims for vets affairs. That means that you are a pretty big player. We want the Australian Federal Police to be absolutely and utterly secure, and it is important that they are. But you, along with Centrelink, are a major player, I would have thought, in relation to the sort of information that somebody might like to access. I noted that you are not connected to Fedlink, but you are accredited for Gatekeeper; is that right?

Dr Richards—That is correct.

CHAIRMAN—Can you tell us why in both cases?

Dr Richards—HIC, as a Commonwealth statutory authority, not as a public service department, is not considered to be part of the Public Service, and it has never been considered a requirement that HIC be part of Fedlink.

CHAIRMAN—But you do fall under the CAC Act.

Dr Richards—We do.

CHAIRMAN—Absolutely.

Ms O'Connell—Just to amplify that, we do not see any drivers or needs at this point in time to use Fedlink. Typically Fedlink is used internally within government agencies in communicated information.

CHAIRMAN—Has Gatekeeper been positive?

Dr Richards—Yes. HIC, in going in the e-business direction and using the Internet as the platform or one of the channels for communication between our customers and HIC, has established public key infrastructure. The arrangements under which the public key infrastructure has been introduced have been fully accredited under Gatekeeper. So that includes the establishment of a registration authority wholly owned by HIC called the Health eSignature Authority. All of the contractual arrangements between HeSA, HIC and the certification authority and with the users of the public key infrastructure—in particular health care providers, doctors and pharmacists—have been accredited through the Gatekeeper process.

CHAIRMAN—If my memory serves me correctly, you are responsible for allocating Medicare numbers?

Dr Richards—Yes.

CHAIRMAN—Which are pretty universally used now throughout the health care system. If you want any kind of service, you need a Medicare number to start with. How frequently does that numbering system get corrupted?

Ms O'Connell—I am not aware of any instances where that numbering system has been corrupted per se, Mr Chairman.

CHAIRMAN—No-one comes in and uses a false number and gets away with it?

Dr Richards—The Medicare number is an administrative arrangement instituted by HIC. In establishing Medicare, the numbering system was really just a shorthand for the name, address and date of birth of individuals to identify them within electronic systems. The Medicare number is now used for a number of HIC related processes—Medicare obviously and the Pharmaceutical Benefits Scheme—to determine entitlement, and it is used to identify children through the

immunisation register. Under the Privacy Act, numbers issued by one government agency are not allowed to be used by another agency for another purpose. So as far as I am aware, Medicare numbers are generally used for identification of an individual in relation to an HIC program.

CHAIRMAN—You said 'generally'. I notice you picked that word quite determinedly.

Dr Richards—Some state governments, in determining eligibility of an individual for public hospital services without charge under the Commonwealth-state health care agreements, under the Australian health care agreements, occasionally seek evidence of eligibility for Medicare prior to acceptance. So even though no claim is generated for an HIC related rebate, the number is recorded in some state public hospital records for the purposes of determining eligibility.

CHAIRMAN—Do you ever run an external test of the security of that numbering system—that is, have somebody attempt, on your behalf, to break into it and allocate numbers or put in a corrupt number? Have you ever tried to prove that you are good enough to prevent that?

Dr Richards—Certainly the physical and logical security of HIC's IT systems are, we believe, sufficient to prevent an external party utilising HIC systems to fraudulently allocate a number or generate a number. We are aware of some forged Medicare cards that were seized in Western Australia I think late last year that were apparently produced in South-East Asia. But they were not, as we understand, forged for the purposes of falsely obtaining Medicare benefits, but more to provide evidence of identity for another purpose.

CHAIRMAN—Are you familiar with the document entitled *Australian government use of information and communications technology: a new governance and investment framework*? It is Management Advisory Committee report No. 2?

Ms O'Connell—Yes, we are.

CHAIRMAN—You participated in this?

Ms O'Connell—Yes, we did, and we certainly support it; and some of the actions following it we are participating in as well.

CHAIRMAN—Do you think creating a more federated structure will limit your ability to do your own thing?

Ms O'Connell—It refers to support for a federated approach on a cooperative basis rather than a mandating basis. So we do not see it in that sense as limiting, but rather taking a more cooperative stance across government where there are reasonable benefits in taking a federated approach. So at this stage we do not see it as being restrictive.

Ms PLIBERSEK—Has anyone tried to break into your system? If so, how regularly does it happen and are they generally the same sort of people just having a go, or do you think there have been specific efforts to get into your system to obtain information?

Ms O'Connell—To my knowledge we have never had a denial of service attack—an attack which has resulted in complete denial of service. We do monitor, of course, all attempted accesses to our Internet services and sites.

Ms PLIBERSEK—But they would just be the same sort of thing that happens to most people?

Ms O'Connell—That is right, viruses, potential viruses and all the rest of it. That is right.

Dr Richards—We have had our Internet gateway accredited by—

Ms O'Connell—By DSD; and we have a fully protected level Internet DSD approved gateway.

Senator LUNDY—Can you describe the process involving the Health eSignature Authority and its relationship with Gatekeeper accreditation?

Dr Richards—The Health eSignature Authority is a wholly owned subsidiary of HIC established solely for the purpose of being a registration authority under the Gatekeeper public key infrastructure arrangements. The role of HeSA, Health eSignature Authority, is to undertake getting evidence for identity checks for people seeking a digital identity issued under the Gatekeeper-approved PKI that HIC has sponsored.

Senator LUNDY—What software do you use for your authentication?

Dr Richards—For the public key infrastructure?

Senator LUNDY—Yes.

Dr Richards—We originally used digital certificates issued by Baltimore. About 12 months ago Baltimore sold its Australian operation to SecureNet. So now we issue SecureNet certificates.

Senator LUNDY—As far as health's IT outsourcing program goes, how much of the management of security related issues is effectively handled by IBM GSA or subcontractors thereof?

Ms O'Connell—In relation to our outsourcing arrangements with IBM GSA, the types of services under that are infrastructure services, so the asset ownership is with IBM GSA, as are the services to operate, run and maintain those infrastructure assets. In terms of security, the HIC retains responsibility for the management of security, and certainly IBM GSA provide some security related services for us under that arrangement.

Senator LUNDY—I am very interested in the sort of demarcation between what IBM GSA do and what you do through your employees, and also the nature of the contractual requirements and any obligations IBM GSA have in relation to what they do.

Ms O'Connell—The contractual obligations on IBM GSA also impose some very stiff sanctions, the stiffest one of course being termination of the contract if they fail to live up to some of their contractual obligations.

Senator LUNDY—The security related contractual—

Ms O'Connell—Security related. It covers a broader gamut than that. It covers clauses to deal with compliance with the Archives Act, data security, confidentiality of our information—the protected use and handling of that is covered—privacy and compliance with the Privacy Act, and also a range of compliance procedures that we have stated in the contract as well.

Senator LUNDY—Does the contract require that IBM GSA comply with all aspects of the Protective Security Manual?

Ms O'Connell—Yes, it does, that is right—that and also another standard, ASCI-33. Both of those are reflected in the contract in terms of their obligations.

Senator LUNDY—As far as reporting goes, in the contracts what requirements are there on IBM GSA to report to you and/or to DSD, given that is non-compulsory?

Ms O'Connell—IBM has a requirement to report to us immediately any security or information breach. Within the HIC, with HIC management of the contract, we do the reporting to DSD under that sort of non-mandatory arrangement at the moment, but we basically report any attempted breach, virus or whatever to DSD under those arrangements.

Senator LUNDY—So it is HIC'' policy to report to DSD?

Ms O'Connell—That is correct, yes.

Senator LUNDY—The whole issue of security and outsourcing certainly was put under the spotlight by the Humphrey review of IT outsourcing. From your experience, are you able to make any comment or observations about what aspects of security really need to be strategically managed in house and which responsibilities are more effectively outsourced?

Ms O'Connell—In constructing our outsourcing arrangements we took into account that the responsibility for security still needed to rest with the Health Insurance Commission. As a result of that we probably have some clauses in our contract that might be a little stiffer or more punitive than other agencies in dealing with privacy of data and confidentiality of information. So we took a very direct approach in safeguarding those arrangements. The balance between what is contracted out with IBM and what remains with the HIC is very much the sort of operational work that is with IBM Global Services, and they have very strict reporting obligations to us on that operational work. In that sense, we feel that is probably the best that it could be made under the present arrangements.

Senator LUNDY—Have you ever had to apply a sanction to IBM GSA because of noncompliance with security, privacy or protection related responsibilities under their contract?

Ms O'Connell—No, we have not. We keep them very aware of their reporting obligations, and certainly as soon as anything happens they are very quick to alert us. That is our experience.

Dr Richards—HIC requires all its staff to undergo privacy training on commencing work with HIC and at regular intervals. IBM GSA staff are also included in that. We recently completed a round of privacy training for IBM GSA staff, so they fully understand their obligations.

Ms O'Connell—But before IBM GSA staff work on our account they are required to obtain a protective level clearance through the ASBS vetting process.

Senator LUNDY—So what proportion of your IT staff would be on contract, through IBM GSA at least and other contractors associated with that, and in house, if you like, from a strategic management point of view?

Ms O'Connell—In relation to the division of what is in house versus outsourced, what is outsourced is our infrastructure services. What remains in house is our application development, our IT planning, our architecture, our quality assurance and testing facilities, our business and IT planning. All of that remains in house. It is the infrastructure services that are contracted out through IBM Global Services. I would have to get the exact numbers for you. In terms of IBM GSA staff working on HIC, they are not always full time, but they require the protected level clearances even if they are to do only a few days work for us essentially. I could get the numbers of IBM GSA staff if you would like them.

Senator LUNDY—Yes, relative to departmental staff; that would be useful. This committee has asked a lot of questions about the perceived relative merits of open source versus proprietary software. To what extent has the Health Insurance Commission investigated the use of open source, or to what extent do you actually use it? I know IBM have made some very public announcements about their close relationship with open source. Have you looked at it? Are you using it?

Ms O'Connell—We have looked at it and we continue to look at it. We do not have use of much open source at all at this point in time. It is interesting that most proprietary providers say that open source has great security vulnerabilities and the open source people suggest that it is the reverse: it is proprietary software that is most vulnerable.

Senator LUNDY—That is a pretty fair reflection of the views that have been put before this committee.

CHAIRMAN—We have discovered that, if anyone did not know it already.

Ms O'Connell—Yes, two different schools of thought, and I do not think I would particularly vote either way at this point as to who might be right and who might be wrong.

Dr Richards—Prior to adopting any form of software, we subject it to testing to ensure that it is fit for purpose.

Ms O'Connell—That is right. All of our systems go through some very rigorous testing.

CHAIRMAN—You said 'much open source'. Where do you use it?

Ms O'Connell—We do not have open source in any of our major areas in terms of operating systems. The reason I caveated that is you never say never. There will be some small piece of open source, but it will be a very minor use within the commission and not for major operational systems. We are, however, quite interested in looking at Linux. There are financial benefits in pursuing Linux in terms of licensing arrangements. Whilst it is proprietarily owned, it is considered open source. It falls perhaps in a new category of definition. But we are quite interested in pursuing that.

Senator LUNDY—It is still commercial applications, if you like, derived from open source.

Ms O'Connell—Yes. So we are interested in looking at that from obviously the financial benefits point of view. We are well aware that it is starting to get much more extensive use within the Commonwealth.

Senator LUNDY—In previous hearings we heard various witnesses refer to HIC and the work it is doing. Optus commented on the level of security required for their Internet connections—and I will quote from the transcript:

As our submission points out, in the case of Optus there is no recognition, for example, of the security features of our private secure Internet—

presumably a VPN that they can provide—

it is simply treated as the public Internet. That means that an expensive solution ... needs to be implemented. Our submission goes into a bit of detail about an arrangement we have had with the Health Insurance Commission. In that instance, the HIC was not able to use our carrier grade security controls and procedures as the Commonwealth does not view them as appropriate. We had to include an accredited T4 security facility and, in our view, that added unnecessary costs.

If you could respond to that now, that would be great; otherwise, could you take it on notice and provide the committee with the Health Insurance Commission's perspective on what Optus is referring to there?

Ms O'Connell—Yes, I can answer that now, if you would like. We have recently engaged Optus as our data network service provider. In terms of gateway and Internet facilities, we mentioned before we have a DSD accredited gateway service. We see that as essential, as part of the government and the business that we undertake. I think Optus would prefer us to apply a lower standard. We chose not to.

Senator LUNDY—When you say 'gateway', that is your security through the interface of the Internet, through a web interface?

Ms O'Connell—Correct, the external firewall. We call it our corporate gateway, yes.

Senator LUNDY—Would the people who use that be both Health Insurance Commission clients, citizens, as well as employees and providers of—

Ms O'Connell—Certainly employees in terms of access through email and browser facilities, the general public in terms of accessing our website, but also providers, most importantly, in terms of the security arrangements for providers.

Dr Richards—For lodgment of claims on Medicare or PBS.

Ms O'Connell—Yes, online.

CHAIRMAN—Everything is encrypted?

Ms O'Connell—Yes.

CHAIRMAN—You cannot have a firewall without everything being encrypted.

Dr Richards—Yes. HIC does take these issues very seriously. It goes fundamentally to HIC's reputation and the trust of the Australian community in the health programs that we administer. So we do all appropriate things to make sure that we are not likely to be subject to a breach. We also periodically engage external consultants to try to hack into our gateway and do real-life testing.

CHAIRMAN—You are not implying that you are perfect?

Dr Richards—No, but we have not had a breach yet, and we take very seriously our desire not to have a breach and we do implement all necessary—

CHAIRMAN—That is very good.

Ms O'Connell—And we will continue to be diligent, obviously taking note that there are advances in technology and advances in the spirit of hackers as well—what they can achieve.

CHAIRMAN—Remember that just because you have a monopoly does not mean that you can get sloppy.

Senator LUNDY—That is not a political statement, is it?

CHAIRMAN—No, it was not a political statement at all.

Senator LUNDY—That is very inappropriate, Chair.

Dr Richards—We are subject to the secrecy provisions of the acts under which we operate, and they are put in there by parliament to emphasise the need to maintain trust in the way in which we manage personal information. We take that very seriously.

Ms PLIBERSEK—When you say that you have had no breaches you mean no-one breaking in from outside, but have you had cases of your own staff inappropriately accessing information intentionally?

Ms O'Connell—Yes, we have, and we have a code of conduct covering staff that they are asked to sign as part of their employment with the HIC. And we have taken action where those events have occurred.

Ms PLIBERSEK—Without being too specific, can you tell us what kind of information staff were trying to access, what action was taken against the staff and at what stage you picked up the transgression?

Dr Richards—There have been a small number of instances of a variety of grades of severity. A number of staff have been dismissed for certain activities. On occasions staff have—there have been newspaper reports of this when it has gone to court and through the legal process—browsed through information either—

Ms PLIBERSEK—About neighbours and—

Dr Richards—Yes, ex-partners—for just general interest, for gossip type interest or for some sort of personal reason.

Ms PLIBERSEK—Sometimes in motor registries people look up addresses and sell them to private investigators. Have you ever had that happen?

Dr Richards—Not that I am aware of.

Ms O'Connell—Not that we are aware of, no. We do check and monitor. All of our staff access to all of the systems is logged, so there is a complete log.

Ms PLIBERSEK—And they know that?

Ms O'Connell—They know that.

Ms PLIBERSEK—So I guess there is an incentive not to do it.

Dr Richards—Every time you log onto the system there is a notice on the screen that comes up and reminds you of your obligations to access information for only purposes related to your employment.

Ms PLIBERSEK—Have you had anyone recently involved in any of that sort of intentional breaching of your code of conduct?

Ms O'Connell—Not I think in the last six months or so in relation to access to data, and Dr Richards will correct me if I am wrong there, but we have more recently had some other forms of misuse—for example, misuse of the Internet, which is also covered by the code of conduct.

Ms PLIBERSEK—Do you mean looking up pornography?

Ms O'Connell—Yes, for example.

Ms PLIBERSEK—It just amazes me that people do that knowing how closely those sorts of things are monitored and tracked in most workplaces now.

Dr Richards—And we again advise staff that we do monitor.

Ms O'Connell—It is covered in the code of conduct as well.

Dr Richards—We scan people's hard drives looking for information of that type.

Ms PLIBERSEK—You have software that does that?

Ms O'Connell—Yes.

Senator LUNDY—Is the software across the Internet that I was talking about before MINS or something different?

Ms O'Connell—MINS stands for Managed IP Network Services, and that is the new data carriage service that we have signed up to with Optus. So that is for our complete internal network. We have 226 Medicare offices around Australia. We have moved from a frame relay technology service to a managed IP service with Optus. That connects to all of our 226 Medicare offices.

Senator LUNDY—That is a virtual private network?

Ms O'Connell—That is correct, yes.

Senator LUNDY—So that is different from the online interface?

Ms O'Connell—That is correct.

Senator LUNDY—I just wanted to clarify that. Is HIC a part of the data-matching legislation?

Dr Richards—Yes.

Senator LUNDY—In terms of identity management and common identifiers, does HIC have its own unique identifiers or does it have a system where HIC and other agencies and departments are now using common identifiers?

Dr Richards—HIC manages its own unique identifier. The Medicare card number is not unique.

Senator LUNDY—No, that is right.

Dr Richards—You are on your parents' card when you are young, then you get your own card and then you go onto your partner's card; and you can be on more than one card at one time.

Your presence on any Medicare card is logged back to a unique identifier. That unique identifier is not shared with any other Commonwealth agency.

Senator LUNDY—My understanding is that it cannot be unless there is some legislative base. Is that your understanding?

Dr Richards—That is my understanding.

Senator LUNDY—The data-matching legislation provides for scenarios where you can provide or share information?

Dr Richards—Under strictly controlled circumstances for limited periods, and the data are then destroyed. We examine each instance of that in great detail prior to engaging in those exercises.

Senator LUNDY—That legislation and any regulations associated with it stipulate specifically—

Dr Richards—And we adhere to those to the letter.

CHAIRMAN—I have two hypothetical questions. If the government's proposed legislation to allow online claiming of Medicare benefits at a doctor's surgery passed the Senate and became law, what sorts of practical difficulties would that cause you in the security environment?

Dr Richards—HIC already provides that type of service, and we have designed that type of service using the public key infrastructure accredited by Gatekeeper to ensure the protection and security of the information that is transmitted.

CHAIRMAN—Are you telling me that all the operational procedures will involve operations at the doctor's surgery or at a hospital, and beyond that your systems are already set up to be able to cope with all that?

Ms O'Connell—Online claiming is in fact already in place and is taking place now. That is one of the primary uses for the Pki, as Brian said. So it is in place now.

Dr Richards—There are a number of channels available to consumers and providers to submit claims to HIC under a variety of programs, and online claiming is an available channel at the moment for those who have—

CHAIRMAN—How do you they do it?

Dr Richards—Through their practice management software, which is integrated with our Pki.

Ms O'Connell—The HIC has produced an API, an applications programming interface, and provided that to the practice management software vendors for them to incorporate in their software, which is typically used at the administration or reception desk in a GP practice, and that is where the claiming takes place.

CHAIRMAN—Is it often used?

Dr Richards—Currently only a small number of software vendors have incorporated this, so there is not an extensive use of online claiming at the moment.

CHAIRMAN—That is what I thought. I did not realise there was any. From time to time it is proposed that every individual's health history be on a national database which has limited accessibility. You are not unaware of these proposals which arise from time to time. What major problems would that cause you?

Dr Richards—Under the Privacy Act individual Australians have a right to access information about themselves held by HIC, and we do provide information to individuals who request that information. We currently do that on paper. The difficulty in providing online access for individual Australians to HIC data comes down to the security and the authentication of the individual. So at the moment we do not provide individual Australians with online access to their data, primarily because we are very concerned to ensure the privacy and security of that information.

CHAIRMAN—If it did eventuate so that you could test your own history and/or you could authorise your doctor or the doctor you are visiting to access your health file, one of the claimed benefits would be that you could go from Dr A to Dr B—because you happened to be in another city, or you had moved to another city or another location, or you had been overseas and had come back, or you had decided you did not like your doctor any more, or you could not get an appointment on time or whatever—and, instead of being asked a giant series of questions by the doctor you are now visiting, who knows nothing about you, they could simply somehow get access to your health file. Wouldn't that create monumental security problems for you?

Dr Richards—HIC has built a system that allows that to occur within the constraints of the coordinated care trials. The second round of the coordinated care trials is yet to commence. But citizens who elect to participate in the coordinated care trials provide specific, informed consent to allow providers to access information held by HIC in an online environment.

CHAIRMAN—Some of the difficulties I am thinking of include not only approval by the individual that their data could be released but also who has authorisation to receive the data, to access the information online.

Dr Richards—That is right. We have looked at technology that would assist in the management of those sorts of complex arrangements.

Ms O'Connell—I think it is less about the technology being the limiting factor and more about the issues associated with managing a person's identity and being sure that when you provide that access it is for the person whom they say they are. I think they are essentially the issues.

CHAIRMAN—I would have thought so, yes. I do not disagree with you, but I would have thought that was a huge challenge.

Dr Richards—A number of countries have embarked on some pilots that do this sort of thing, and there are two ways in which this is currently being managed internationally, to my knowledge. One way is in some countries the individual patients are provided with a smart card with a digital certificate that they need to insert in the smart card reader in the practitioner's office to directly authorise access to their personal information. Other arrangements are that the practitioner simply states that they have the consent of the individual, and that is subject to audits. In some of those cases the patients are provided with access to logs of who has accessed their data and under what circumstances. There are penalties that can apply for inappropriate or fraudulent access by providers.

CHAIRMAN—It is thought to be a highly sensitive area, isn't it? I do not care who knows my health history. It does not worry me one way or another. It does not bother me in the slightest. But there are individuals who believe it would limit their vocational choices, their sporting or artistic choices—all sorts of things. It is seen as needing probably the most secure privacy arrangements around.

Dr Richards—Generally where these sorts of trials have been implemented they have been done on the basis of an informed consent, opt-in process so that patients deliberately and overtly consent to having their data available in these ways.

CHAIRMAN—Under limited circumstances.

Dr Richards—Under limited circumstances. Therefore, if you do not wish your data to be accessed, you do not participate in those activities.

CHAIRMAN—But it would require some very austere management.

Dr Richards—It certainly requires the technology. Certainly audit trails and access logs would be a fundamental component of any such arrangement.

CHAIRMAN—Thank you very much. I assume if we have any further questions you will not mind if we put them to you in writing.

Ms O'Connell—We would be happy to take them.

CHAIRMAN—Thank you very much for coming today.

Ms O'Connell—Thank you.

[11.14 a.m.]

CAMPBELL, Ms Kathryn, First Assistant Secretary, Social Welfare Division, Department of Finance and Administration

FLAVEL, Mr Matthew James, Branch Manager, Budget Coordination, Department of Finance and Administration

LOUDON, Mr Mike, Branch Manager, Procurement, Department of Finance and Administration

NICHOLSON, Mr John, Branch Manager, Infrastructure Branch, Department of Finance and Administration

STAUN, Mr Dominic, General Manager, Financial and e-Solutions Group, Department of Finance and Administration

STINZIANI, Mr Antony, Branch Manager, Strategy and Service Management Branch, Department of Finance and Administration

CHAIRMAN—I welcome the representatives of the Department of Finance and Administration appearing at today's hearing. Thank you very much for coming to talk to us today. We have no submission from you, but would you like to make a very brief opening statement?

Mr Staun—We understand you want to cover a range of subjects, so I have taken the liberty of bringing along a range of people. Hopefully we can answer all of your questions to your satisfaction.

CHAIRMAN—That is good. In 2001 you were one of a number of agencies subject to a performance audit by ANAO, as reported in Audit report No. 14 2002-03: *Health group IT outsourcing tender process*. Can you tell us the results of that audit and where we are going?

Mr Staun—No, Mr Chairman, I do not have any knowledge of that. In what regard were we subject to—

CHAIRMAN—DOFA was the subject of an ANAO performance audit, reported in Audit report No. 14 2002-03: *Health group IT outsourcing tender process*. It was not still OASITO then.

Mr Loudon—I think so, yes.

Mr Staun—So this was to do with OASITO, was it, in that period?

CHAIRMAN—OASITO was not still around then, was it?

Senator LUNDY—I think it was at the time that tender process was concluded.

CHAIRMAN—Okay, forget the question.

Senator LUNDY—I think OASITO's demise was during the period of the audit.

CHAIRMAN—We will not proceed down that track any further.

Senator LUNDY—Although there might be some questions relating to outsourcing generally of security issues.

CHAIRMAN—Sure; I will leave those to you. I understand that Dr Watt was a member of the management group that produced Management Advisory Committee report No. 2, *Australian government use of information and communications technology: a new governance and investment framework*, which talks about federation principles in terms of operations across government departments and outside federal agencies that respond to or are subject to the CAC Act. Have you been involved in that process, or are you involved?

Mr Staun—Yes, certainly Dr Watt is a member of the MAC. In terms of whole-of-government IT and so on, I ask Antony Stinziani to speak to that.

Mr Stinziani—We are certainly aware of it, and, as you said, Dr Watt was involved. Dr Watt is a member of the IMSC now, and I am a member of the Chief Information Officers Council. We support the report in its current format, and we are also a member of a number of working groups that came out of that report. One of them is to do with second-generation sourcing.

CHAIRMAN—My understanding is that, while the Public Service Act supports all department CEOs and individual agency CEOs—secretaries, whatever they are called—being totally responsible for their operations, nonetheless the further we move down the line in this devolved environment—of course it is the old central command environment—we seem to be moving back towards some centralisation. Your department is very much involved in that, particularly with things like purchasing and writing standards across the Commonwealth. Have you seen departments changing what they are doing as a result of this overall consultative approach?

Mr Staun—In relation to IT?

CHAIRMAN—Yes, and IT security particularly.

Mr Staun—First of all on the procurement side—

Mr Loudon—In general on IT procurement I think with the formation of the IMSC, the Information Management Strategy Committee, and the CIOC we are seeing evidence of sharing of more information more formally and feedback into Finance about what is happening. In general procurement policy we are not seeing any particular flowthrough other than a more cooperative approach across agencies.

CHAIRMAN—Our understanding from talking to a number of agencies so far has been that a number of them seem to be moving away from outsourcing all their IT and going back to doing IT in house partially or completely. Can you comment on that?

Mr Staun—I think the whole of the outsourcing industry over the last five years, not just restricted to the public sector but also in the private sector, has seen pluses and minuses with the process. Certainly a selective sourcing model or best of breed approach and so on is gathering favour. That might mean a combination of different outsourcers rather than a single tier 1 provider across the whole of the range of applications and hardware. It might also mean for specific towers bringing it in house.

CHAIRMAN—How about DOFA?

Mr Staun—We are in the process at the moment of putting together a team for our infrastructure sourcing project. We have a contract with IBM GSA which expires in November 2004. We, as part of that process, will be looking at the types of sourcing options that are available to us, including all three of those, that is a full tier 1 service provision or various towers or indeed in house. We are not restricting ourselves to any one particular model at this stage.

CHAIRMAN—Why are you, as a leading government agency, not connected to Fedlink?

Ms Campbell—I am not sure what the Fedlink is.

CHAIRMAN—You are kidding, aren't you?

Mr Staun—I think we will ask Antony Stinziani to tell us what Fedlink is and then we can—

CHAIRMAN—Are you serious?

Mr Stinziani—I know what Fedlink is. There are a number of initiatives that are being worked through that NOIE are coordinating, and we support those. Gatekeeper is another example. We do not necessarily have a full business requirement to move ahead and take advantage of the work that has been done just yet. But, in saying that, we are not ruling it out.

Senator LUNDY—Fedlink is primarily, as I am sure you are aware, an interdepartmental secure connection. If you do not use Fedlink, how do you exchange information securely between the department of finance and other agencies and departments?

Mr Stinziani—The main system we have is the accrual information management system, AIMS. At the moment we are working towards the budget estimates framework review, which Kathryn and Matthew might be able to expand on slightly. We will be looking at our requirements and then assessing whether Fedlink, Gatekeeper et cetera are appropriate for our requirements down the track. At the moment we have a system in place that has been in place for some time, and it is meeting our security obligations at the moment.

Senator LUNDY—Does AIMS run on a dedicated network or a virtual private network?

Mr Nicholson—It is a virtual private network.

Senator LUNDY—Can you tell me what level of security you have on it? Do you have the accredited T4 secure facility on that network, on that VPN?

Mr Nicholson—Was the question does it run at that level?

Senator LUNDY—Yes.

Mr Nicholson—No, it does not. It runs in confidence level.

Senator LUNDY—I am presuming the Commonwealth Protective Security Manual identifies these different levels of security. Can you confirm that it would be because the department of finance has determined that that level of security is adequate for that purpose and it is still in accordance with the manual?

Mr Stinziani—I believe so. Our security policy is consistent with the PSM.

Senator LUNDY—I know you are locked into a contract with IBM GSA, but what scope has there been within your existing contract for DOFA to consider the use of open source software—whether it be some sort of commercial form of open source software? Has there been any scope?

Mr Nicholson—There has been very little scope to date. Effectively, under the contract with IBM GSA, they are required to provide the software source and they have chosen to use a Microsoft product rather than an open source product. As Mr Staun mentioned, we are about to go back out to the market for an ongoing service provider, and in that context we may well look for options for other than a straight proprietary system of software.

Senator LUNDY—Under your current contract with IBM GSA, how specifically do you evoke the security standards? We have heard from other departments and agencies that obviously that is a mandatory aspect of the contractual obligations. Is that the case?

Mr Nicholson—Yes, it is. It is the case.

Senator LUNDY—Have you ever had to apply a sanction to IBM GSA for a security related—

Mr Nicholson—No, we have not.

Senator LUNDY—What do they call them—service credits, failure to meet their service level agreements, breaches, whatever?

Mr Nicholson—We have had to impose service credits but not for a security breach, no.

Senator LUNDY—So they have a clean record in that regard?

Mr Nicholson—Yes, they do.

Senator LUNDY—As far as the reporting requirements are concerned, again the committee has heard that it is not compulsory for agencies and departments to report to DSD any security incidents. What is DOFA's policy?

Mr Nicholson—We have a policy of reporting all such incidents directly to DSD should they occur, and we have reported them regularly in the past when there has—I would not say they are regular but quite often there are attacks of one nature or another which are of concern and we immediately report them to DSD.

Senator LUNDY—Has DOFA ever experienced an incident like a denial of service attack and so forth that qualifies as definitely a reportable incident but one that has perhaps caused you to reflect on your policy as well?

Mr Nicholson—We get many attacks, but none of them has been successful to date, and that is why we are confident that the security mechanisms that our service provider have in place are hitting the mark.

Senator LUNDY—What about some of the worms and viruses that circulate from time to time? How robust is your system in fending them off and not letting them in? If you use Microsoft software, you are probably vulnerable to SQL Slammer. How did you fare with SQL Slammer in January?

Mr Nicholson—I cannot give you a direct response to that, Senator. I am not sure of the specific answer to that particular issue. More generally, again there are regular virus attacks that are usually rebuffed. The last one that I can recall that was an issue was the 'I love you' virus, which managed to permeate its way through the department. But, to my recollection, there has been none since then that has been successful.

Senator LUNDY—What are the department's policies in terms of managing its environment internally—proactive monitoring of emails, of the use of the Internet?

Mr Stinziani—We have an Internet and an email policy in place, and we do regular monitoring certainly on Internet access.

Senator LUNDY—Do you filter email or the Internet? For example, do you apply any filters to the World Wide Web?

Mr Stinziani—I do not believe so.

Mr Nicholson—No, we do not; but we monitor, again on an irregular basis, the usage of the Internet.

Senator LUNDY—Do you apply any spam filters to the department?

Mr Nicholson—Yes, we do.

Senator LUNDY—How do they work?

Mr Nicholson—Mixed.

Senator LUNDY—What is your rating?

Mr Nicholson—Mixed. We have very effective blockers against unacceptable material such as pornographic material. They are less successful against some of the companies around town that seem to spring up on a daily basis, I suspect, wanting to sell us their wares. It is very difficult to preclude those. Once we have found one that is offensive or indeed in any way unacceptable, we preclude that particular organisation from accessing our email. But they just grow up seemingly on a daily basis and it is very hard to control that.

CHAIRMAN—'You don't know me, but I want to be your friend because I have a million dollars for you.'

Mr Nicholson—That is the type. We have had a few of those. A couple of Nigerian gentlemen have contacted us.

CHAIRMAN—A few! I get 20 a day.

Senator LUNDY—With respect to DOFA's management of the endorsed supplier arrangement, I guess it is primarily IT related, but, more broadly, what security considerations does DOFA apply to companies seeking endorsed supplier status?

Mr Loudon—There is no specific requirement under the rules for ESA in relation to security. We look at performance. The main criteria are in relation to financial viability: a record of performance, particularly in the government sector—mainly around those issues. There is no specific one on security. We would expect any issues in relation to suspect companies to be evident probably through the references that we apply against those companies and/or whether there had been something registered with, say, ASIC or something similar in relation to their performance. We do those sorts of checks in relation to their reliability as a company but not specifically in the area of security.

Senator LUNDY—In terms of ESA and IT companies, what degree of breakdown do you apply to companies applying for ESA status? Do you make a distinction between different subsectors within IT? Is there a group that is about security and critical infrastructure protection?

Mr Loudon—In the system there is a significant number of products and services. It is able to be categorised by companies applying, self-nominating in the areas in which they sell products and services. In relation to system access, that narrows down what buyers would be able to look for. We check that in relation to the initial endorsement—what they are selling, how much have they sold before. In the IT industry obviously you need to continue to develop those listings as companies continue to change their products and service mix. We also have a review mechanism whereby those things are monitored over a three-year rolling program. That is across everything that we check, including their incorporation and their financial viability. There are just so many products available and so many services. We do try to keep an up-to-date listing, but it is difficult, and we try to categorise.

Senator LUNDY—But you cannot point to anything under perhaps a security category where there are additional checks based on the capabilities of the companies?

Mr Loudon—Not directly in relation to the service other than the references, no.

Mr Nicholson—But certainly, as part of the normal tendering process and the evaluation of those tenders, we go through quite a rigorous analysis of the company's financial viability and its technical capacity et cetera.

Mr Loudon—The prequalification arrangements are very much around taking some of the issues out and looking at them up front, such as references and financial viability in particular. But in relation to specific services, because of the large variety particularly in IT and the moving feast, individual agencies need to be in control of that particular aspect.

Senator LUNDY—There are a whole range of standards emerging, such as for the archiving of electronic information. Can DOFA nominate any standards that they apply to storage of electronic information or guidelines that they adhere to in that regard? I am happy for you to take that question on notice. My understanding from evidence so far is that different standards are emerging—for example, ebXML—for database style information but also storage of information that does not necessarily need to be accessed on a daily basis but certainly needs to be kept.

CHAIRMAN—And how do you get it 20 years from now?

Senator LUNDY—That is the issue. We are seeing agencies and departments have those expectations placed upon them in accordance with their legislation, but quite often the standards applied are highly proprietary and therefore it is questionable whether or not people will get access in 20 years time. So there are those kinds of issues. Please take on notice the general question about your policies in that regard, what stage they are at and whether they are formative at this stage or under discussion.

Mr Nicholson—I recall a discussion recently in POITAG—Senator Lundy, I am not sure if you were there or not—that related to the same issue in terms of members and senators and their data.

CHAIRMAN—What was that?

Mr Nicholson—It was a discussion in POITAG, the Presiding Officers Information Technology Advisory Group, which Senator Lundy is a member of, that was discussing the same issue.

Senator LUNDY—Yes. I just make the observation that, when parliamentarians use Microsoft products, the back compatibility of the document software is notorious. In fact, it is a device used to stimulate the purchase of new software, but you have to maintain back editions as well. On that note, what is the primary platform used within DOFA? You mentioned Microsoft before.

Mr Nicholson—Yes. We operate on a Microsoft server platform for desktops and a UNIX based platform for our midrange systems. The operating systems are currently Windows 2000, and we use the Microsoft Office suite of products.

Senator LUNDY—Are you also looking at the .NET platforms? Is that something DOFA is considering?

Mr Nicholson—We will look at it in the context of our revised sourcing. We have a policy of adopting software X minus one. To use terminology that Dominic Staun would use, we would rather be on the leading edge than the bleeding edge. So we have a policy of waiting until the—

Senator LUNDY—So you will not be going to XP just yet?

Mr Nicholson—Not immediately, but we may well go to XP or .NET in the context of the revised arrangements that will take place from November of next year.

Senator LUNDY—Is DOFA in a position to make any observations about the relative merits of the security of the software that you are currently using as compared with open source or indeed other proprietary software packages and platforms?

Mr Nicholson—I am not personally able to. It would be only hearsay or my reading of the market and the technology. We do not have any personal experience of it within the department, given we are a Microsoft shop effectively.

CHAIRMAN—So you operate on all open source systems?

Mr Nicholson—We do not. We operate on Microsoft proprietary systems by and large.

Mr Staun—I presume you are talking about Linux and these sorts of systems.

Senator LUNDY—I am talking about Linux and UNIX, but also the commercial applications of both. I think there is a tendency to assume that open source means that no external provider is involved, when quite often there is and there are lots of different scenarios in between one or the other. What about disaster recovery and redundancy in your information technology systems?

Mr Nicholson—Under the contract with IBM GSA, they are required to provide the department with a disaster recovery plan. They have done so and we have accepted it and it is in place. Separately, we are undertaking right at this time a review of our total disaster recovery and business continuity capacity. From that, we expect to be making some short- and medium-term changes to our disaster recovery arrangements.

Senator LUNDY—In relation to that whole gamut of privacy, security and critical infrastructure protection, I would like to know about the effect of the whole-of-government guidelines, the sort that have been prepared by NOIE from time to time—or, according to NOIE, circulated by NOIE but prepared collectively. Because you have been locked into an IBM GSA contract for some time, what kind of imposition has the increased awareness about security related issues had on that contract's terms and conditions? Has it resulted specifically in any

variations to that contract, either negotiated variations or additional contracts with other security related IT firms?

Mr Nicholson—Not to my knowledge. Mr Stinziani may wish to talk to this, but we have quite recently moved to remove a significant part of the security environment outside the bounds of our current service provider—that is the provision of the firewall services, which we have removed, with IBM GSA's concurrence, from the existing contract—and have now gone to the market.

Senator LUNDY—Why is that?

Mr Stinziani—It is really in line with a move to getting full DSD accreditation to a protected level, which is what we require.

Senator LUNDY—IBM GSA could not provide that, or were they asking for too much money?

Mr Nicholson—Neither, actually. The subcontractor that IBM GSA had doing the work did not have DSD accreditation for its product and was not likely to get DSD accreditation in the foreseeable future. So it was our view that it was unacceptable to continue with that arrangement.

Senator LUNDY—So what prompted DOFA to make that decision to change, to find someone who could provide you with the upgraded—and I presume this is for the Internet interface aspects of your work—

Mr Nicholson—The firewall, yes, that allows data to come into the department. It was our view that to not have a DSD accredited firewall was unacceptable.

Senator LUNDY—That is not a mandatory condition, is it?

Mr Nicholson—No, it is not.

Senator LUNDY—So it is just a policy decision within the department?

Mr Nicholson—Yes.

Mr Stinziani—We like to be as consistent as possible with DSD's policy.

Senator LUNDY—Do you think it would be useful or helpful or both for that requirement to be mandated, either within a regulation or legislation?

Mr Staun—I guess we could not see any problem with it. Certainly we comply with it and would comply with it. I think it makes a lot of sense to do that.

CHAIRMAN—But might not there be other smaller departments—

Mr Staun—That is what I was thinking.

CHAIRMAN—that do not play outside the Public Service environment.

Mr Staun—That would be the consideration.

Ms PLIBERSEK—Was it expensive for you to comply?

Senator LUNDY—No; was it expensive for you to do it?

Mr Nicholson—It was expensive in the short term to take the decision to move to another provider. But we believe the long-term solution will be not only a DSD accredited but also a cost-effective solution.

Ms PLIBERSEK—Where will the savings come from?

Mr Nicholson—We think we can do a better deal, if you like, dealing directly with the company—whichever company we seek to do the deal with—than we were under a subcontracted basis with IBM GSA.

Senator LUNDY—Did you have to pay IBM out any money?

Mr Nicholson—No. We came to a mutual agreement.

Senator LUNDY—That would have to be a first.

Mr Nicholson—I should qualify that. We agreed with IBM GSA that we would pay them for the reasonable costs of moving away from their service provider arrangement. So any unavoidable costs that they had to bear we agreed we would pay, but there were no additional costs or charges.

Senator LUNDY—Contractual penalties?

Mr Nicholson—No, no penalties.

Senator LUNDY—You are in the process of finalising that contract?

Mr Nicholson—Yes. We are in the process of finalising the tendering process.

Senator LUNDY—So you have not selected a provider as yet?

Mr Nicholson—Not fully.

Mr Stinziani—We have not signed a contract yet.

Senator LUNDY—You cannot tell me whom it is? You do not have to.

Mr Nicholson—I do not believe so.

Mr Staun—We will be signing the contract very shortly. We will let the JCPAA know at that point in time.

Senator LUNDY—I am just curious.

Mr Staun—We will let you know.

Senator LUNDY—In providing that new firewall service to you, what security requirements that were not originally in the IBM GSA contract will you include in this one?

Mr Nicholson—To my knowledge, there are no additional requirements other than it will meet the DSD accreditation.

Mr Staun—It will allow us better internal monitoring and so on of usage through the Internet and so on, which will obviously be good from a policy implementation viewpoint.

Senator LUNDY—Just to pick up on that point, the Humphrey review, which I am sure you are familiar with in the post IT outsourcing program environment, identified security and strategic control of security issues as major issues. The model you have just described I think is strong evidence that departments which have previously followed the model are now identifying security as something special, strategic, and actually pulling it out of those contracts. Is that a fair observation?

Mr Staun—Yes, I think it is a fair observation. As I said earlier, I think people have learnt through the sourcing process and that, quite typically, one size does not fit all. Organisations like IBM, for instance, have particular skills in this one area and not in another, and particularly if you are then subcontracting to a third party to provide security you would have to ask yourself whether that is really the way it should operate. It can well operate in that way by having a tier 1 operator, but equally it can operate well by dealing directly, if that is part of the sourcing arrangement which you wish to go to. I can see advantages in both. I think people are realising that 'pick and choose' and so on is the way to operate.

Senator LUNDY—The other questions I have are more about policy directions of the government Advisory Management Group in relation to IT. Are you in a position to answer questions about that? It is the whole-of-government document that the chair referred to earlier.

Mr Staun—To the extent that we are able to, yes.

Senator LUNDY—It relates to DOFA in the sense of cost efficiency, which has been a significant motivator of the involvement of the Department of Finance and Administration in how government agencies and departments source their requirements. What do you see as the imperative cost issues emerging out of the second generation sourcing model? Do you think they had as primary a weighting as they did previously given the heightened security environment and the lesson learnt from the previous outsourcing model? Does anyone want to have a go at that?

Mr Loudon—In relation to the models that we are seeing emerge from this sort of work, the flexibility that the system has and people are taking account of through the use of second sourcing, looking at the agencies' needs, and the costing functions arising given quite significant changes in the security environment, both globally and nationally, and within data itself, are coming to the fore but looking at what is best needed by particular agencies. So in many ways I think we are seeing a natural progression of how costs will be dealt with, what importance security has in relation to overall departmental need, what strategic functions that relates to and therefore what are the systems that support those functions. I think the roles of the IMSC and the CIOC are coming to the fore. One of the great advances of those bodies has been to be able to look at what is happening at the individual agency level, bringing that into an environment of cooperation and seeing whether the same issues are emerging. So cost is only one of the functions. I think what we are seeing is need progressing and then costs being examined.

Senator LUNDY—As opposed to cost being the driver.

Mr Loudon—Yes.

Senator LUNDY—And needs being secondary.

Mr Loudon—In particular in this area, the strategic output of better security, what you are employing it to do, the last thing that government would want is to see a knee-jerk reaction to security issues. So consideration of exactly what you are protecting, why you are protecting it and the ability at chief executive level to respond to that need I think is emerging. But recognition that you cannot do that without talking to your colleagues and looking at what is happening and emerging with IT, it being a particularly dynamic sector—the processes of software now will not be around in five years, much less 10 years or 20 years—and the ability to be able to share experience, build on what is happening in the market and understand what the market is offering across the whole sector I think are part of the new environment. But it is definitely not just cost that is driving the issues.

CHAIRMAN—Is it fair to say that to sit still in that sort of environment is to go backwards?

Mr Loudon—I think the environment has not changed in that regard.

CHAIRMAN—Hansard cannot respond to heads shaking up and down.

Mr Loudon—Yes. The environment in the rapidity of change has not changed in IT. It just changes focus every so often. This year it is security.

CHAIRMAN—Ultimately the world.

Mr Loudon—That is right.

Ms PLIBERSEK—Can I ask a question not about your technology but about your personnel. Have any of your staff accessed information they have not been authorised to access? What happens when that happens?

Mr Staun—Like accessing an inappropriate site on the Internet?

Ms PLIBERSEK—Tell us about the Internet and that stuff as well, but people looking up records that they do not have authorisation to look up, for example.

Mr Staun—All applications are covered by various degrees of password control, access and so on. So, as a general statement, no, I am not aware of any particular issues that have come up of unauthorised access within the department to staff records or anything like that. With regard to the Internet, yes, there have been issues of inappropriate access. They have been picked up through our systems, and management action has been taken.

Ms PLIBERSEK—You use some software filtering system that picks up—

Mr Staun—Yes, monitoring.

CHAIRMAN—Thank you very much for coming. If we have any further questions, you will not mind if we put them in writing rather than having you come back.

Mr Staun—Not at all.

CHAIRMAN—I think you owe us an answer to at least one question that you took on notice.

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

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

CHAIRMAN—I thank our witnesses, our observers, secretariat staff, my colleagues and, last but definitely not ever least, Hansard.

Committee adjourned at 11.53 a.m.