COMMONWEALTH OF AUSTRALIA

Official Committee Hansard

JOINT COMMITTEE OF PUBLIC ACCOUNTS AND AUDIT

Reference: Management and integrity of electronic information in the Commonwealth

THURSDAY, 26 JUNE 2003

CANBERRA

BY AUTHORITY OF THE PARLIAMENT

JOINT COMMITTEE OF PUBLIC ACCOUNTS AND AUDIT

Thursday, 26 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, Mr Cobb, 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

Committee met at 11.14 a.m.

DE LA MOTTE, Mr Geoff, Manager, Information and IT Technology Services, Department of the Treasury

ROBINSON, Mr Ian, General Manager, Corporate Services, Department of the Treasury

CHAIRMAN—The Joint Committee of Public Accounts and Audit will now continue taking evidence, as provided for in the Public Accounts and Audit Committee Act 1951, for its inquiry into the management and integrity of electronic information in the Commonwealth. I welcome everyone here this morning to the committee's sixth public hearing of this inquiry. Today we will hear evidence from the treasury department. Before commencing proceedings, I advise witnesses that hearings today are legal proceedings of the parliament and warrant the same respect as proceedings of the House itself. The giving of false or misleading evidence is a serious matter and may be regarded as a contempt of parliament. The evidence given today will be recorded by Hansard and will attract parliamentary privilege. Finally, I refer any members of the press who are present to a committee statement about the broadcasting of proceedings. In particular, I draw the media's attention to the need to report fairly and accurately the proceedings of the committee. Copies of this committee statement are available from secretariat staff. I now welcome representatives from Treasury. Thank you very much for coming and for your brief submission. Would you like to make a brief opening statement?

Mr Robinson—No, there is nothing more we wanted to add.

CHAIRMAN—That is good. In 2001 you took part in the ANAO performance audit of Internet security which led to our inquiry. What was the outcome of that audit with respect to Treasury?

Mr De La Motte—As I understand it, the Internet security audit focused on web sites and the security surrounding web sites. On that occasion, a number of issues were raised with Treasury about a couple of web sites that were developed externally. During and as a result of that audit, we upgraded the security on those web sites and, as I recall, Audit was happy with the work that we had done. Since that time, we have applied web site design security standards to everything we do. So it was a positive outcome for Treasury. We got to fix some things and we got to upgrade what we were doing.

CHAIRMAN—That is good. I can say on behalf of the committee that we are pleased to hear that, because we have a view that Audit adds value and most of the people around this place now agree with us. There is still the odd person who gets very touchy because they did something wrong or did not do something well enough and they feel they are being criticised by Audit, but that is tough. That is part of the business of being accountable. Do you have any interaction with DSD?

Mr Robinson—Yes, we do. Our IT network is accredited by DSD, so that is the major contact that we have. We had them in to accredit the gateway to our network 12 months or so ago. I understand we are due to be reaccredited later this year.

CHAIRMAN—You will be accredited later this year for FedLink?

Mr Robinson—We are now on FedLink.

CHAIRMAN—You are on FedLink?

Mr Robinson—Yes. We connected to FedLink just prior to the budget this year, so in May.

CHAIRMAN—What do you use it for?

Mr Robinson—Because it is still quite new, we have not developed our use of it fully, but our revenue group in particular will be using it to communicate with the Office of Parliamentary Counsel on legal drafting type issues. In time, as more people join FedLink, we will use it for secure communications with a wider range of agencies.

CHAIRMAN—What about communications with Finance when you are doing budget preparation?

Mr Robinson—Yes, that is another opportunity. We already have, I understand, a pre-existing link to Finance that we have used to date.

CHAIRMAN—Is it secure?

Mr Robinson—Yes, it is encrypted.

CHAIRMAN—There are no leaks?

Mr Robinson—No, not from that source.

Mr De La Motte—It is in the form of a dedicated network between the two departments.

CHAIRMAN—It is not open source; it is closed source.

Mr De La Motte—It sure is.

Ms PLIBERSEK—Does that mean you have to dig your own trench and lay your own wire?

Mr De La Motte—Or you can hire your own phone line.

Ms PLIBERSEK—So you have hired a phone line?

Mr De La Motte—Yes. With the encryption that goes with it as well, it is highly secure.

CHAIRMAN—You said that you will be accredited to use Gatekeeper?

Mr Robinson—Yes. That is correct—

Mr De La Motte—We will be accredited to—

CHAIRMAN—Not to use Gatekeeper, but you will be accredited by Gatekeeper?

Mr De La Motte—Yes, to the protected level. We would not necessarily use Gatekeeper that often, but we are certainly complying with it.

CHAIRMAN—How will you use it? Who will be impressed by the fact that you have that level of security?

Mr Robinson—I guess our main concern is to ensure that our network, and the information on it, is protected. Obviously, Treasury deals with a fairly large amount of classified information, including commercial-in-confidence information. So our objective has been just to protect the security of the information we have. With respect to Gatekeeper itself, I guess we do not expect to make major use of Gatekeeper because we do not see our operations requiring that.

CHAIRMAN—Have you had many instances of people breaking into your secure communications?

Mr Robinson—Very few. We had two instances in 2000. The committee members may recall that we had one instance where a page on the Treasury web site was corrupted, and that was as a result of a flaw in the Microsoft code we were using at the time. The web site was taken down, it was corrected and a security patch was applied. The other occasion was in relation to the GST Start-up Assistance Office. In that case, there was a database that was externally developed and externally hosted and there was a flaw in the code which allowed a hacker, if you like, to access the confidential information of people who had applied to that office. Again, the site was taken down immediately and the code was fixed.

CHAIRMAN—Were you under contract to IBM at the time for your code development?

Mr Robinson—No.

Mr De La Motte—No.

CHAIRMAN—You did it internally?

Mr Robinson—The GST Start-up Assistance Office development was contracted out to an external supplier. Aside from those two instances, we have had no intrusions.

CHAIRMAN—Do you still contract out or do you do it internally?

Mr Robinson—We do a lot of it internally. We do contract out some applications but, of course, we supervise those very closely and make sure they comply with all our standards.

CHAIRMAN—Once bitten, twice shy? Would Hansard please note that Mr Robinson nodded his head yes.

Mr KING—Well said, Chairman.

Ms PLIBERSEK—Following on from what you said about the development and the maintenance of web sites being contracted out, is that predominantly what you do? Do you normally do them in-house or do you normally contract them out?

Mr Robinson—It is a mixture. We try to do them in-house where we can, but it is a resourcing issue and sometimes—particularly if there is a time constraint—it is more efficient to contract them out.

Ms PLIBERSEK—I remember that the example to do with the GST Start-up Assistance Office made it into the newspapers at the time.

Mr Robinson—Yes.

Ms PLIBERSEK—I presume you write penalties into your contracts for such breaches?

Mr Robinson—Yes, that is correct.

Mr De La Motte—We certainly write warranty requirements into that and fix that up. We do include that liquidated damages clauses must be agreed to. In other words, if the work they do causes us a loss, we can then claim to the value of the contract.

Ms PLIBERSEK—You cannot really quantify the damage to your reputation in a situation like that. It was the banking details, wasn’t it, of 17,000 businesses?

Mr Robinson—That is right.

Ms PLIBERSEK—Are you able to tell us how quickly you picked up the problem, whether any bank accounts were actually accessed at the time and basically what the consequences were of that security breach?

Mr Robinson—I understood it was picked up very quickly and that there were no bank account details accessed. As I understand it, the hacker actually sent back to applicants details of their bank accounts. His objective appeared simply to be to expose the weakness in the scheme rather than to exploit it.

Ms PLIBERSEK—Lucky for you.

Mr Robinson—Indeed.

Mr De La Motte—The details that he did send back were bank account numbers. There was nothing else with regard to the account and nothing you could look inside at.

Ms PLIBERSEK—If someone’s aim in that situation had been to access people’s bank accounts to transfer money from those bank accounts into one of their own, would that have been possible?

Mr De La Motte—I do not think so because most people’s bank accounts are password protected, if you are doing it through the electronic medium. I doubt they could have accessed the bank account details at a transaction level.

CHAIRMAN—It is true, isn’t it, that if you throw away your bank statement somebody could find it in the tip?

Mr Robinson—That is quite right, yes.

Mr De La Motte—The banks have a regime of security that is set up to stop people coming in and accessing other people’s bank accounts, even if they know the numbers. There are a lot of verification procedures.

Ms PLIBERSEK—I want to ask you about archival integrity. We have spoken to a number of departments about their varying views of what type of computer language they want to use so that in 50 years time they are not depending on Microsoft still being a company or any of these types of businesses continuing. Have you given thought to how you retain electronic information for archival purposes, the kind of language you use and how that data is physically stored?

Mr De La Motte—For archiving information, we follow the National Archives’ guidelines in relation to their business classification scheme, which defines naming conventions to the information that you will save. At the data end of things we are following a standard convention, so it should not be too difficult to search and find out what we have. In terms of the language that it is stored in, we are a Microsoft organisation. This information would be held on proprietary software called TRIM that Treasury is installing at the moment. That is a preferred supplier to the government, is used extensively throughout Australia and is making inroads throughout the world. We have not thought down to the level that you are talking about because we are fairly comfortable that we are not using anything unusual that might put us in a situation of not being able to access information in later years.

Ms PLIBERSEK—Can you remind me what the language was that some of the other government departments were talking about using?

Secretary—PDF or XML.

Ms PLIBERSEK—I think the argument was that XML was, in the end, the more basic thing that would be readable by more—

Secretary—PDF is in the same situation as Microsoft; it is commercial software. So, if the originator goes out of business, you have the same problem. XML is open source.

Mr De La Motte—Yes, we are moving into XML. We have been using HTML, hypertext mark-up language. But we will be using XML, extensible mark-up language, more in our web sites. To get to that, we will start using that more extensively when we upgrade our operating systems and our desktop software, where XML is more of a feature. We are on Microsoft Office 97 at the moment on our desktop. We are moving up to XP.

Ms PLIBERSEK—When you have finished with information now, do you just store it in whatever program it has been created in? You do not make any efforts to store it in a way that ensures its readability in 20 or 30 years time? Do you understand the distinction I am making?

Mr De La Motte—Yes. Treasury is implementing proprietary software called TRIM Context. We have implemented it across the corporate area and a number of other areas so far. That is a common information warehouse, if you like—a formal storage area.

Ms PLIBERSEK—Can you explain that to me a little bit? Does TRIM Context read documents that have been created in the past in a different way? I do not understand what it does, I am sorry.

Mr De La Motte—It is an official electronic filing system, if you like. When documents are created, authors are required to save them into that, following those business classification scheme guidelines. Because it is an official filing system, that is where we capture all our vital records—records that evidence how decisions were made. We capture emails, Word documents and spreadsheets. It will gradually take the place of the old paper filing system.

Ms PLIBERSEK—So that is like a filing system that is on your mainframe, is it, and every person who sits down at a computer in the treasury department files into that same system?

Mr De La Motte—Eventually.

Mr Robinson—It will be eventually. We are just in the process of developing this and rolling it out.

Ms PLIBERSEK—But that will not capture documents that have been created in the past? When it is implemented, it will just be documents from that time on?

Mr De La Motte—We could. If we found that we were implementing this software at a time when a project or a policy development was half finished, we could scan in documents that were created in a paper format to make the electronic file complete. We also provide a link in the electronic system which identifies the numbers of the paper files that were used previously on that topic.

Mr JOHN COBB—At what stage do you involve the Federal Police? At what stage do you say, ‘This is a breach breaking the law’? How do you determine when you involve them?

Mr Robinson—I guess a judgment call is made, depending on the severity of the breach.

Mr JOHN COBB—So you do not necessarily do it?

Mr Robinson—Not automatically, no, but there have been very few occasions in the past where we have needed to face up to that issue.

Mr JOHN COBB—Because it has not been a breach of law?

Mr Robinson—Yes.

Mr JOHN COBB—But, if there were a breach of law, would you automatically involve the Federal Police?

Mr Robinson—Absolutely, yes. On broader, non-IT related issues, obviously if we think there is a criminal issue involved we would call in the Federal Police.

Mr JOHN COBB—So simply breaching your defences is not a criminal issue?

Mr Robinson—As I said, apart from those two instances on web sites that I have mentioned, we have not had any breaches in nearly the last five years. So I guess we have not had to face up to that issue.

CHAIRMAN—Senator Lundy?

Senator LUNDY—I am in serious danger of traversing the same ground that you have just traversed.

CHAIRMAN—While Senator Lundy is gathering her thoughts, I will ask a few questions. The Management Advisory Committee, of which Dr Henry, Secretary to the Commonwealth Treasury, is a member, released its report entitled *Australian Government Use of Information and Communications Technology: A New Governance and Investment Framework*. Did Treasury participate in the development of that document?

Mr Robinson—We did not have an active involvement, no.

CHAIRMAN—Are you happy with it?

Mr Robinson—Yes, we have no difficulties with that document.

CHAIRMAN—Do you think the outcomes generated by the report and the degree of cooperation across the Commonwealth agencies should have positive outcomes?

Mr Robinson—I would expect so, yes. The Management Advisory Committee has been a useful tool across quite a range of corporate issues. I think it is a very good development. It allows departments to share experience and reach common views on best practice.

CHAIRMAN—Now I will ask you a very difficult question. Do you think at times we go a bit overboard in the way we approach IT security? Have we, because of the odd glitch like the two you have told us about, become a bit paranoid?

Mr Robinson—That is a difficult question. You have to make a case-by-case judgment. Clearly, security is not costless, and it will always be a case of assessing each particular situation and making a judgment on how much security is required and whether the cost fits into a sensible risk-benefit equation. It is always easy to be wise after the event. A degree of risk management is involved in all of these questions.

Mr De La Motte—We are reminded daily of the exposures that we can have in the electronic medium by our monitoring of activity on our firewall in our Internet gateway, where we observe multiple attempts at intrusion every day. There are also emails containing viruses hitting our firewall and getting knocked back. We monitor that and have a report every morning. We are certainly reminded of how busy the world is out there in trying to intrude on people's—

Ms PLIBERSEK—How many do you get a day?

Mr De La Motte—I had a message the other morning that we had had five attempts at viruses coming in. The average would be about three.

Ms PLIBERSEK—What about people trying to hack in?

Mr De La Motte—There are multiple attempts—30 or 40, that sort of thing.

Ms PLIBERSEK—Can you tell from your system whether they are just sweeps or whether they are people making a concerted effort?

Mr De La Motte—Yes, we can. We are required to report the concerted effort to DSD.

Senator LUNDY—Through ISIDRAS?

Mr De La Motte—Yes. They want to be able to follow those up if they recognise that that is occurring on many government sites.

Ms PLIBERSEK—Are you happy with the feedback that DSD give you? Once you provide them with that information, do they give you enough feedback or help to overcome the problem if there has been an actual breach?

Mr De La Motte—We have always found them very useful, especially when they involve themselves in audits. Like we mentioned before, the Audit Office will often bring DSD in with them. As was said before, we do not have many particular problems that come from that. We advise DSD that we have had attempts at intrusion, they take it away and they look at it. They do not necessarily come back to us and report on every instance, but we have fulfilled our responsibility by letting them know. We find DSD very useful in a lot of ways.

Senator LUNDY—Do you think the reporting requirements, such as the ISIDRAS system, should be mandatory for all agencies and departments, or—speaking for yourself—a mandatory system?

Mr De La Motte—My first reaction is to say yes, because it would then result, hopefully, in all agencies dealing with issues in the same way. There has to be some strength that comes from that, especially for DSD. Having all the information reported in the same way would probably make it easier to recognise a solution covering all agencies.

Senator LUNDY—I want to go back to something that occurred some years ago involving the provision of a CD-ROM of information to the Commonwealth Bank and Dun and Bradstreet, from memory, as part of a pilot for them to cross-reference their ABN numbers into the system—

CHAIRMAN—They did all that.

Senator LUNDY—I am not sure this is the same occurrence, so I am just checking. The one that I know you have referenced is another matter.

This was the provision of a CD-ROM effectively at cost to both of those organisations for the purpose of some sort of pilot—that was the reason the government gave. I raised it in Senate estimates as being a fundamental breach of privacy principles. Again, this is from memory as I have not looked at the *Hansard* recently, but the government's defence at the time was that this was part of a cost recovery service that the government had engaged in in collating large tracts of data—in this case, it was companies and their ABN numbers—and selling that on a cost recovery basis to other organisations that had a strong relationship with or a purpose that I presume somehow supported or a common interest in the government's objectives. I use that as the context to ask the question: are there any overarching policies that you apply to your department in relation to the availability of bulk data—either about constituents' businesses or any other aspect of your business—on a cost recovery basis, for sale to actually make money or for free?

Mr Robinson—I do not recall that particular instance. Was that involving the Treasury?

Senator LUNDY—No, it involved the ATO.

Mr Robinson—To answer your generic question, I guess we do not typically provide bulk data to the public or to a client base. If we did, we would abide by the privacy principles. We are obviously obliged to abide by those principles.

Senator LUNDY—Thank you for that. The next question I have—and this was raised at the time—is that, if you did provide that information according to all of the privacy guidelines but the organisation you provided it to did not abide by them, where would the liability fall?

Mr Robinson—I cannot answer that. That would be a legal question that I would need to pursue. I do not recall any instances where we as an organisation have provided that sort of data. It is not really in the nature of our business.

Senator LUNDY—I will not go any further with it, but it raises issues about the integrity of Commonwealth data, although from a slightly different perspective to that of a breach of databases or information systems having occurred.

Mr De La Motte—Most of the information that comes out of Treasury is in the form of a publication. We do not get requests of the sort that you are talking about. Something coming out in a publication is all very controlled. The other way we publish is on our web sites. We choose to give out only certain types of information. Indeed, with the types of requests we get I doubt that would arise. You could say that if we were asked about that we would look at the issue on a case-by-case basis, and we would be looking for controls and assurances that were relative to the particular information that was given.

CHAIRMAN—Thank you very much for coming to talk to us today and, again, thank you for your submission. If we have any further questions, would you mind if we put them to you in writing so that you do not have to come back again?

Mr Robinson—No; please do.

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, I thank my colleagues and I thank the secretariat staff. Last but not least, God bless Hansard.

Committee adjourned at 11.45 a.m.