
COMMONWEALTH OF AUSTRALIA

# Official Committee Hansard

## JOINT COMMITTEE OF PUBLIC ACCOUNTS AND AUDIT

**Reference: Management and integrity of electronic information in the Commonwealth**

FRIDAY, 17 OCTOBER 2003

CANBERRA

BY AUTHORITY OF THE PARLIAMENT

**INTERNET**

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

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

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

**JOINT COMMITTEE OF PUBLIC ACCOUNTS AND AUDIT**

**Friday, 17 October 2003**

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

**Senators and members in attendance:** Senator Lundy and Mr Charles, Ms Catherine King and Ms Grierson

**Terms of reference for the inquiry:**

To inquire into and report on:

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

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

In conducting its inquiry the Committee will consider:

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

**WITNESSES**

**Committee met at 9.09 a.m.**

**CHAIRMAN**—The Joint Committee of Public Accounts and Audit will continue taking evidence, as provided for in the Public Accounts and Audit Committee Act 1951, in its inquiry into management and integrity of electronic information in the Commonwealth. I welcome everyone here this morning to the committee's seventh public hearing of this inquiry. Today we will hear evidence from two departments that have recently suffered serious breaches of computer security and from several agencies directly involved in coordinating security issues and investigating security breaches. Before commencing proceedings, I advise witnesses that the hearings today are legal proceedings of the parliament and warrant the same respect as proceedings of the House itself. The giving of false or misleading evidence is a serious matter and may be regarded as a contempt of parliament. The evidence given today will be recorded by Hansard and will attract parliamentary privilege. Finally, I refer any members of the press who are present to 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 the secretariat staff.

[9.11 a.m.]

**SMITH, Mr Michael, Executive Director, Australian Federal Government Group, EDS Australia**

**CHAIR**—Welcome. We were very disappointed to find, in the course of another inquiry, that two servers—which sounds rather innocuous but they are huge computers in their own right—had been stolen from the Australian Customs Service facilities at Mascot, which led us to reopen this inquiry. We had been, in a sense, negligent in not asking people how well they physically secured their IT equipment—in fact, we had not asked them at all—but, by the same token, no-one volunteered any information either. At the beginning of those hearings, I read out a statement about not giving false or misleading evidence. I cannot say that anybody gave us false or misleading evidence—they just did not give us the evidence. This more than annoyed us, I can tell you. Michael, do you want to tell us about that event at Mascot?

**Mr Smith**—We clearly need to be careful when discussing the details surrounding that event, because the two people who have been charged with regard to that event are currently going through proceedings in Sydney courts. My understanding is that two men entered the Customs premises at the Charles Ulm building at Mascot late in the afternoon of 27 August. They presented themselves as contractors and gained access to a secured room that contained telephone PABX equipment and some spare PCs that we used to replace PCs around the offices—around that area where there were problems with those PCs. They disconnected the two servers and related peripheral equipment, placed them in a trolley that was in the room and left the building.

**CHAIRMAN**—Do you have the equipment back?

**Mr Smith**—EDS does not have the equipment back. It is currently being held as evidence.

**CHAIRMAN**—The Commonwealth has the equipment back.

**Mr Smith**—Yes, the equipment has been recovered.

**CHAIRMAN**—Did the Australian Federal Police do that?

**Mr Smith**—That is my understanding, but I am not sure. The matter is before the local Sydney courts.

**CHAIRMAN**—We have worked our way through this inquiry worried about worms, viruses and all sorts of other cyberspace attacks, but they pale into insignificance if somebody can walk in and steal a mainframe.

**Mr Smith**—I think it is most probably appropriate to say that it was not a mainframe; it was a server.

**CHAIRMAN**—With the greatest of respect, that is what it was. They are massive computers in their own right.

**Mr Smith**—Yes, they are significant computing devices; I would agree with that.

**CHAIRMAN**—Thank you. Isn't that of major concern?

**Mr Smith**—Certainly it is of major concern, I would agree. If I were to take a look at the matters that the committee was hearing before, certainly a lot of the investigation and focus of the computer industry, and in particular the computer security industry, is related to logical security all basically trying to stop attacks on networks. However, there is an assumption that physical security around key systems is going to be in place. If we take a look at the incident that occurred, EDS considers that there was a strong and robust security process and policy in place within Customs. But there was a local practice in place that was not in accordance with Customs security, and that practice was allowing people into a room unescorted and clearly without sufficient evidence of who they were. I would say that the approach being taken within Customs, defined by the policy and processes that were in place, was sound, robust and sufficient to secure that equipment. What occurred was a breakdown in that process. My understanding is that that has subsequently been addressed, but it certainly is a concern.

**CHAIRMAN**—Whose responsibility is it for security at that site?

**Mr Smith**—The security at that site is the responsibility of Customs.

**CHAIRMAN**—I understand that one of the people who stole the equipment was an EDS employee and that one was a subcontractor for EDS.

**Mr Smith**—I was not aware of the second piece of information that you gave, but one of the gentleman who has been charged was, until earlier this year, an employee of EDS.

**CHAIRMAN**—What sorts of security controls or otherwise do you have over your subcontractors, your sub-subcontractors and your sub-sub-subcontractors?

**Mr Smith**—Anybody providing services to the Commonwealth as part of EDS or as a subcontractor to EDS or as a subcontractor to one of EDS's subcontractors is required to go through a similar set of security checks. In fact, one of the things that I believe has been an improvement in security since the introduction of outsourcing within the Commonwealth is that there is a tighter observance of the requirement to clear people who are doing work for the Commonwealth.

**Senator LUNDY**—I would like to get some clarification. The Commonwealth has been outsourcing for about 100 years.

**Mr Smith**—I mean for ICT outsourcing, so from the late 1990s.

**Senator LUNDY**—Under the government's IT outsourcing program that started in 1997?

**Mr Smith**—That is correct.

**Senator LUNDY**—There was a lot of IT outsourcing before then as well.

**Mr Smith**—Yes, I understand that.

**Senator LUNDY**—So it was the government's program, and you say they initiated improved security checks.

**Mr Smith**—There were improved security checks that were implemented at that time. I could go through some supporting evidence for that. One of the things that anybody who is providing services is required to do is to go through a government-sponsored vetting process. When EDS took responsibility for the clients that we took responsibility for, the majority of the people who were in the agency and transferred over to EDS were not cleared. In at least one instance, one of the people we took responsibility for was unable to pass the clearance and therefore was unable to deliver services. There is a comprehensive vetting process which is being observed now because of the increased scrutiny on the service delivery.

**CHAIRMAN**—You had problems at other agencies? You do work for other Commonwealth agencies, don't you?

**Mr Smith**—Yes, we do—the Child Support Agency and the Australian Taxation Office. We have not had problems similar to this. I think it is fair to say that, as part of our delivery of services, there are a lot of items that are much more attractive and portable—like laptop computers and mobile phones—and those things are stolen and lost from time to time. But there is no secure data on those devices.

**Ms KING**—Could you say how many have been lost over the course of your contract?

**Mr Smith**—My understanding is that there is a protocol in place within government now whereby the agencies report those numbers. I guess that would be a matter that would be best answered by the agencies.

**Senator LUNDY**—I want to go back to the issue of physical security. Are the requirements for physical security of information technology contained in the *Protective Security Manual*?

**Mr Smith**—There are three documents. If we take a look at our requirements under our contracts that we have at the moment, each of the agencies has a security policy, and we need to be in accordance with that policy. In addition, there are two key government documents: one is the *Protective Security Manual* and the other is ACSI 33. Those are the things which define what we need to achieve in terms of our—

**Senator LUNDY**—So adherence with the guidelines in the *Protective Security Manual* and compliance with ACSI 33 are effectively conditions of your contract?

**Mr Smith**—That is correct.

**Senator LUNDY**—In terms of the incident that occurred at the airport, and the theft, were there any measures identified where EDS was found to be in breach of either the PSM or ACSI 33?

**Mr Smith**—I am not aware of any.

**Senator LUNDY**—Has there been an investigation?

**Mr Smith**—There have been a number of investigations. My understanding is that they are not complete—

**Senator LUNDY**—Investigations by whom?

**Mr Smith**—There are a number of internal investigations within the government, and I am not privy to the reports for those. They are cabinet-in-confidence, I believe, so I have not seen those. What was established immediately following the incident occurring: Customs have a process to establish a Customs incident response committee to address the incident. EDS was a member of that. One of the things that we are doing is making sure that we review—

**Senator LUNDY**—Just going back to my question, can you tell me, as a representative of EDS, what inquiries are currently occurring within Customs and within the government, as opposed to police inquiries?

**Mr Smith**—Sorry; I was referring to that. Within the government, there are a number of internal inquiries.

**Senator LUNDY**—Can you tell me what they are?

**Mr Smith**—I am sorry; I am not privy to those. Those inquiries are cabinet-in-confidence—

**Senator LUNDY**—But who is doing them?

**Mr Smith**—I really do not know—sorry.

**Senator LUNDY**—Is it the Department of the Prime Minister and Cabinet? Is it Customs? Who is doing those internal inquiries?

**Mr Smith**—I am not sure.

**Senator LUNDY**—Has EDS had to respond to questions from those inquiries?

**Mr Smith**—There are people in EDS—which has not included me—who have been interviewed as part of the investigation process.

**Senator LUNDY**—But you do not know who is interviewing.

**Mr Smith**—I am not aware of who has been interviewing.

**Senator LUNDY**—Could you take that on notice? I would like to know who is conducting those inquiries.

**Mr Smith**—I am happy to take that question on notice.

**Senator LUNDY**—I think it is a bit odd that you cannot say who is conducting the inquiries. Have EDS conducted their own internal inquiry about the failure in security procedures?

**Mr Smith**—EDS is conducting an inquiry in conjunction with Customs under the Customs incident response committee process.

**Senator LUNDY**—Is that the only inquiry being conducted by EDS?

**Mr Smith**—In addition, EDS has a quality system process and, under the quality system, there is something called a process improvement note. We have established one of those and we are working through the process. That process will not be completed until all of the investigations are completed, to ensure that we understand all of the matters that are affecting us.

**Senator LUNDY**—Again for clarification: the *Protective Security Manual* does cover physical security of IT equipment, does it not?

**Mr Smith**—I believe so.

**Senator LUNDY**—I just wanted to make that point, Mr Chairman. You said earlier that you were concerned that we had not addressed issues of physical security whereas my interpretation of this committee's inquiry is that we have, on a number of occasions, ranged across the *Protective Security Manual* and its application to agencies and departments. I think your point is valid; that is, that the information—

**CHAIRMAN**—We did not ask the questions, though.

**Senator LUNDY**—The information was not offered up, either, when we asked about the implementation and adherence to the PSM. I think that is an important point to make. My next question in relation to EDS is in relation to the contract. Because it is your contract that evokes these standards on how you conduct your work for the Commonwealth government, what contractual remedy or sanction will now be applied to EDS as a result of what has occurred?

**Mr Smith**—I think it is important to understand that the matter we are discussing here is a breach of physical security—so, somebody let somebody in the door and somebody was able to get something.

**Senator LUNDY**—But it is still covered by the PSM, and you are obligated under your contract to comply with the PSM.

**Mr Smith**—Just to clarify responsibilities: the responsibility here for physical security of the site was with Customs; it was not with EDS.

**Ms KING**—You said that the two people who committed this act had presented themselves as contractors. What work did they do that allowed the Customs service to believe that they were contractors? Did they have an EDS uniform? Did they have a badge?

**Mr Smith**—I do not believe that they presented themselves as EDS contractors; I believe they presented themselves as contractors representing another organisation. But, again, that is most probably something that is best asked of the Australian Federal Police.

**Ms KING**—Had the person who was a former EDS employee been in that building before? Was it a common practice for them to be there?

**Mr Smith**—Yes, part of their duties was delivering services to Customs. So they would have been involved in visiting that—

**Ms KING**—So they possibly would have been a familiar face to people in Customs?

**Mr Smith**—Possibly. They most probably would have been in that building at some stage in the past.

**Ms KING**—Do you have any processes to notify Customs or your clients when staff are no longer working for you?

**Mr Smith**—In this instance, there was certainly an understanding between Customs and EDS that this person had left.

**Ms KING**—Do you know who in Customs had that understanding and with whom they had that understanding?

**Mr Smith**—Customs was aware that this person was leaving.

**Ms KING**—Sorry, but Customs is a pretty big organisation.

**Mr Smith**—To answer your question in that case: I do not believe that there is anything in place that would have notified people at the site that that person had left.

**Ms KING**—What sort of staff turnover do you have at EDS?

**Mr Smith**—I can answer generally and, if you like, I can get the exact figures. I believe it would be in the vicinity of around 10 per cent or 12 per cent per year.

**Senator LUNDY**—I want to return to the issue of sanctions. What sanctions exist under the EDS's contract with Customs that could apply to you if you were found—with all these internal inquiries—to have not fulfilled your obligations?

**Mr Smith**—I believe termination of the contract is a remedy for breach of security obligations.

**Senator LUNDY**—Is that the only remedy contained in the contract?

**Mr Smith**—I am unable to answer that, sorry.

**Senator LUNDY**—I am aware that, in some of these contracts, there are other types of sanctions that relate to financial penalties. I think the term used is 'service credits'.

**Mr Smith**—To my knowledge, there are no service credits, but termination is an option. Whenever somebody is buying something, there is always the option of not paying. If you do not receive a service properly, you cannot pay for it.

**Senator LUNDY**—I just want to focus in on this. What is the contract worth that EDS has with Customs?

**Mr Smith**—If you take the amounts that have been publicly listed, for the five years that have gone and the two years that it has been extended, it is worth around $250 million.

**Senator LUNDY**—Were any of the IT assets within Customs transferred to EDS as part of the arrangement?

**Mr Smith**—Yes.

**Senator LUNDY**—So does EDS now own all of Customs' IT assets—like computers, networking equipment et cetera?

**Mr Smith**—I am sure that there are IT assets around Customs that do not belong to EDS but I believe that they would be in the minority.

**Senator LUNDY**—So, effectively, you do own most of the hardware and software?

**Mr Smith**—That is correct.

**Senator LUNDY**—Are you able to put a figure on the value of those assets—approximately?

**Mr Smith**—If we are looking at the value of the assets that were taken, it was less than $3,000.

**Senator LUNDY**—Less than $3,000?

**Mr Smith**—Sorry; the value of the assets that were stolen—

**Senator LUNDY**—I am not talking about the stolen assets; I am talking about overall.

**Mr Smith**—Sorry, I do not have that number.

**Senator LUNDY**—It would be in the millions of dollars, would it not?

**Mr Smith**—Yes, it would.

**Senator LUNDY**—Tens of millions—maybe even in hundreds of millions?

**Mr Smith**—It would not be in the hundreds of millions but it would certainly be millions of dollars worth of assets.

**Senator LUNDY**—So, if EDS are found to have breached their contract and the only sanction that is able to be applied is cancellation of that contract, Customs would find itself in a position of having no assets?

**Mr Smith**—If there is an issue, there are other mechanisms—

**Senator LUNDY**—I appreciate that, but if EDS's contract was terminated and Customs said, 'We no longer require your service,' it would really be up to Customs to negotiate back ownership of those assets, would it not?

**Mr Smith**—That is covered by the contract, so I do not believe that there would be any problems.

**Senator LUNDY**—But they would have to buy it back, wouldn't they?

**Mr Smith**—With the introduction of the government's outsourcing program, one thing that the Commonwealth was very careful about was to make sure that it could not be held to ransom if ever termination was required. Therefore, there are clauses that ensure that, basically, the Commonwealth will not be disadvantaged.

**Senator LUNDY**—So are you saying that the Commonwealth would not have to buy back the assets?

**Mr Smith**—What I am saying is that the Commonwealth would not be disadvantaged.

**Senator LUNDY**—I am asking you whether or not the Commonwealth would have to buy back the assets.

**Mr Smith**—The Commonwealth certainly has the option of buying the assets.

**Senator LUNDY**—So the Commonwealth could take the option of saying, 'Go and take all your equipment with you,' leaving Customs in, what I would put to you, an impossible situation? The point I am making is that the prospect of cancelling EDS's contract is not a particularly credible prospect, particularly in the current circumstances with all of the concern about security and the core role that IT plays. Effectively, that paints a picture of no credible sanction being available to the Commonwealth if security is breached in this way in Customs.

**Mr Smith**—If I can just respond to that: there has been no suggestion that EDS has done anything wrong or contributed to anything that has led to the theft of these devices. I guess I would respond to you by saying that I understand in general terms that you might want to understand some of the details about our contract, but I do not see how it is relevant to the matter that we are discussing at the moment.

**Senator LUNDY**—Is any national security information stored on computers in EDS facilities or on IT equipment that is owned, controlled and managed by EDS?

**Mr Smith**—The highest level information that I am aware of that EDS stores on behalf of Customs, the tax office and the Child Support Agency is highly protected.

**Senator LUNDY**—Public protected?

**Mr Smith**—No, highly protected.

**Senator LUNDY**—Even though you own the vast majority of information technology assets at Customs, you are saying that the highest level of security is highly protected?

**Mr Smith**—I may be wrong, but I believe that to be the case. I can take the question on notice if you like and get back to you.

**Senator LUNDY**—To what extent do Commonwealth agencies that EDS is contracted to store information off site?

**Mr Smith**—All of our agencies have off-site storage arrangements. Those off-site storage arrangements are reviewed in the same manner as the locations where we keep things to ensure that they comply with the security requirements.

**Senator LUNDY**—Are any data or information assets stored offshore?

**Mr Smith**—No.

**Senator LUNDY**—Is that a condition of the contract?

**Mr Smith**—That is a condition of the contract.

**Ms GRIERSON**—You say that these two gentlemen, two thieves, who entered the building did not claim to be EDS representatives. You said they claimed to be from another organisation. What other organisation would have access to the computer equipment?

**Mr Smith**—Within the locked room there are telephone PABXs and other equipment. Again, that is most probably something that is better answered by either the Federal Police or Customs.

**Ms GRIERSON**—But you do not outsource to any other contractors to go to those facilities.

**Mr Smith**—We certainly have some other subcontractors that attend there.

**Ms GRIERSON**—Did you recheck the security checks that you went through for this person who was an employee of yours?

**Mr Smith**—That is right. Prior to anybody commencing work, in this case with Customs, they have to have passed a check. This person passed the check that needed to be gone through, which I believe is conducted by the Security Vetting Service. It is the standard check that all public servants go through.

**Ms GRIERSON**—You are saying that your former employee went through two checking processes: one by you and one by Customs?

**Mr Smith**—That is correct.

**Ms GRIERSON**—So did you revisit the security processes that you had in place at the time? Are you satisfied that the checks you did in employing that person were satisfactory?

**Mr Smith**—Yes, we are satisfied.

**Ms GRIERSON**—How often do you review those?

**Mr Smith**—We have a separate organisation that does that. If you like, I can get back to you with that information.

**Ms GRIERSON**—I think that is important. I would like to know how often that process is audited and whether you do random checks on employees on a regular basis. Did you establish whether your previous employee had handed in their security ID?

**Mr Smith**—Yes, we did. He did.

**Ms GRIERSON**—We have heard of instances where that has not occurred.

**Mr Smith**—A check list is completed for all employees to ensure that we recover all assets, that we remove their access to computer systems and that we collect their passes. That was completed.

**Ms GRIERSON**—One thing that is crucial to this committee is identifying whether the information was the target of the theft of the computers or the hardware. Do you have an opinion on that?

**Mr Smith**—I believe the hardware was the target. Again, that is probably a question that is better asked of the Australian Federal Police.

**Ms GRIERSON**—Thank you. Have you changed your security practices since this incident?

**Mr Smith**—I do not believe there were any weaknesses identified that led to this.

**Ms GRIERSON**—As the major contractor responsible for Commonwealth agency security and computer information, have you submitted recommendations to those agencies on what their responsibilities are? Are there any recommendations that would suggest they should change their practices?

**Mr Smith**—As I mentioned, Customs have established a Customs incident response committee. EDS are a key part of that, and we are making recommendations to them as part of that process.

**Ms GRIERSON**—Thank you.

**Ms KING**—You said before that you thought the hardware was worth about $3,000. It seems like an awful lot of trouble to go to, with potentially harsh penalties, for three grand. Do you want to comment on that at all?

**Mr Smith**—Yes, I agree. It is a lot of effort to go to for devices that are not worth very much.

**Ms KING**—Doesn't that imply that they are after the data and not the hardware?

**Mr Smith**—That is not my view, but again I would suggest that that be taken up with the Australian Federal Police.

**CHAIRMAN**—Thank you very much, Mr Smith. You owe us some answers, so we expect those in writing. We would appreciate your agreement to answer any further questions we have, and if we could put them in writing rather than asking you to come back.

**Mr Smith**—Okay. That would be fine.

**Senator LUNDY**—There is another question here, which is: 'Have there been any other breaches of security involving EDS equipment or at EDS facilities where Commonwealth information is stored?' I would like a response to that.

**Mr Smith**—That was asked, and we gave a response.

**CHAIRMAN**—We have in front of us a list of submissions to this inquiry. Would someone move that they be authorised for publication.

**Senator LUNDY**—I will.

**CHAIRMAN**—If there is no objection, it is so ordered.

**Senator LUNDY**—With respect to the information just published by the committee, I think it is timely to note that the responses by a number of departments—but in particular three agencies which are part of the group 5 contract with Telstra Enterprise Services—have reported what they describe as a serious breach of IT security involving the loss of a quantity of backup tapes by Telstra Enterprise Services Pty Ltd, and that occurred in March 2003. TES is the outsourced information technology and telecommunications service provider for group 5 agencies, of which this department is a member. Other departments that are members include: the Department of Communications, Information Technology and the Arts, the Department of Transport and Regional Services, the Department of the Prime Minister and Cabinet, and the Australian Competition and Consumer Commission. I think that DISR—the Department of Industry, Science and Resources—were the original members of the group 5 contract.

**CHAIRMAN**—We have got to get—

**Senator LUNDY**—I know, but this is incredibly important. What we are dealing with here is a serious breach which has now been formally reported to the committee. What occurred was the

loss of backup tapes, due to a major breakdown in TES's tape handling procedures, and the backup tapes have not been recovered. Both of the responses state that Dr Shergold wrote to Dr Ziggy Switkowski, the CEO of Telstra, to express group 5's extreme concern with the extent of this security breach and the negligence of TES staff in the protection of Commonwealth information. Dr Switkowski assured group 5 that Telstra and TES were very concerned with the seriousness of the breach and had revised the procedures and processes for backup to ensure that all agency information would be handled appropriately, as is required under the contract.

What we have heard this morning is that, under other contracts, the sanction for such a security breach would be loss of contract; so I look forward to the opportunity, through this inquiry, to see what sanction was taken against Telstra in what has been described by agency heads as a serious IT security breach.

[9.44 a.m.]

**LEWIS, Dr Edward James Essington, Convenor, Australian Identity Security Alliance**

**CHAIRMAN**—I welcome the representative of the Australian Identity Security Alliance to today's hearing. Thank you for coming back to talk to us again. I have gone back and reread the transcript of evidence you gave us last time. You made an opening statement in which you said:

... sledgehammer attacks like the one at Customs last week, where somebody breaks in and steals things. They include the several hundred laptops which are lost out of government agencies each year.

I said, 'thousands?' and you said, 'Yes, thousands.' I then said, 'Not hundreds?' and you said, 'We were trying to be conservative.' Do you want to revise your estimate now? Are we talking about hundreds of thousands? From the information that we have received so far from departments, I do not think we have yet had 100 in any one year.

**Dr Lewis**—My recollection of what was said was that you said thousands and I said hundred and then we echoed back.

**CHAIRMAN**—That is not what the transcript says.

**Dr Lewis**—You have it in front of you and I do not. The figures that I was going on at the time were based upon the survey that—amongst others—Senator Lundy carried out, which showed that there were 1,035 in 1999-2000 and 541 from an incomplete survey in the following year. So we are talking somewhere between 500 and 1,000.

**CHAIRMAN**—Is that government agencies or the private sector as well?

**Dr Lewis**—Government agencies only—and only some of the agencies.

**CHAIRMAN**—I said:

So somebody might steal the mainframe?

And you said:

Yes, it has happened a number of times.

Are we talking about Commonwealth mainframes?

**Dr Lewis**—Let me explain one thing. With respect to your use of the word 'mainframe', I would not use the word 'mainframe' in the context of a server. A mainframe is a large machine—a special purpose machine usually. It is equivalent to a freight train; whereas we are looking at things which are more equivalent to panel vans—special purpose machines which are a lot smaller that are used as servers. Of course, laptops are equivalent to utilities or private cars. So,

in the scale of things, I do not know of any circumstances where anyone has stolen a large machine that we would call a mainframe. There have been a number of circumstances where people have stolen servers here and overseas.

**CHAIRMAN**—Of what value would the servers be to them?

**Dr Lewis**—There are two levels of value: one is the physical—the theft for resale—and the other is the damage that is incurred in either restoring the data that was stored on the server or in making for the loss of a server in other ways. For example, the figure quoted just from theft of a laptop—much less a server—is $US89,000. That is from the FBI computer crime and security survey which was carried out in 2002.

**CHAIRMAN**—How is that?

**Dr Lewis**—It is mainly the recovery costs, the restoration of the data that has been lost, the change in procedures, the managerial action and the disruption to the organisation.

**CHAIRMAN**—Have there been any equivalent Australian surveys?

**Dr Lewis**—Not that I know of—not with that level of detail. There are equivalent Australian surveys but, whether they have been looking at that detail with respect to the impact on the organisation, I do not know.

**CHAIRMAN**—You also mentioned, in relation to the aviation security inquiry, that the people in the process are the weak points in the security system. Can you elaborate on that a bit?

**Dr Lewis**—Yes, on two aspects. One is that the need to protect a system depends upon everyone involved in protection being aware of their responsibilities and being trained and skilled in carrying out those responsibilities. That ranges all the way from receptionists on desks, security guards—who do not necessarily belong to the organisation—and of course the members of the organisation itself, up to and including especially the CEO. At the moment those responsibilities are not necessarily supported by adequate training.

**Ms GRIERSON**—You specialise in providing security services, and you have heard the evidence of EDS. What system changes would you recommend, having heard of that incident?

**Dr Lewis**—Before I answer anything about EDS, I need to point out four aspects that might be regarded as colouring my evidence. Apart from being here as Convenor of Australian Identity Security Alliance and the chairman of the Standards Australia committee preparing a standard in ICT governance, in the past I was on the evaluation team which led to the selection of EDS for the Customs outsourcing exercise and, more recently, we have carried out some work on data integrity for the Australian Customs Service. So we have a background in dealing with these organisations in different areas.

To answer the question, perhaps it starts with the role of ICT governance. The recommendation is that the responsibility for security, be it physical or electronic, should be with the CEO. In our view, it is a non-delegatable responsibility. It might be implemented by the technical specialists, who need to be trained or educated in that role—perhaps a slight bias

there—but the buck really is at the top and should be reflected through the layers of management. It is not enough to say to a security guard or to a worker that they need to do better in their job; they also need the resources necessary to do their jobs. That includes training in procedures and practices. As you saw from the evidence before, the breakdown was in a practice. A breakdown in practice comes usually from a lack of training.

**Ms GRIERSON**—Do you have a view on whether the theft of that equipment was information based or equipment based, considering those people spent some time in the building?

**Dr Lewis**—I have suspicions, but they are only hypotheses and not based on any facts.

**Ms GRIERSON**—Do you have any comments to make on penalty systems in contracts?

**Dr Lewis**—Yes. I was involved in the evaluation and preparation of the contract that has been referred to, and we looked at that issue at the time. A security breach is material breach of the contract, which can lead to cessation. As the senator pointed out, major practical difficulties would arise from that. There are the normal commercial legal responsibilities of suing for a breach of contract rather than terminating the contract, so perhaps there are other ways of taking action. That particular contract does not have sufficient service credit or more interim penalties that allow for these sorts of breaches.

**Senator LUNDY**—I am interested in your general views about the increased risk to security of IT as a result of outsourcing. Certainly a number of reports identify that as a key concern, including the independent Humphry review into the IT outsourcing initiative, which recommended that that initiative cease and cited security as one of the reasons. Do you have any comments generally about the impact on security and security risks as a result of outsourcing?

**Dr Lewis**—It is about risk management. I think you raised that issue when we spoke about outsourcing in general some years ago. The role of a contract is important but more important is the role of the contract manager. The contract is only as good as the ability of the agency, in this case, to manage the contract. The risks can increase if the people who are responsible for management of the contract do not know how to. There are examples in other agencies where the contract managers have no background in IT and have no idea of the aspects of the contract they should be paying attention to according to the risk—they really only check that the invoices have been paid, so there is a risk in that area.

If security is a responsibility of an outsourcer, then the contract needs to be very clear about where those responsibilities lie and the people managing their contract need to obviously be in a position to audit to make sure that those responsibilities are being carried out. That involves the sorts of arrangements that are possible now of having appropriate Commonwealth agencies to carry out that audit. If that is part of the contract, if that contract clause is actually exercised—in other words, the contract manager asks for the audit—those risks can be mitigated to an extent. If those things do not happen, the risk continues and the Commonwealth agency has problems with the loss of equipment and the private sector has even more so.

**Senator LUNDY**—In the context of your observations as someone with some expertise in the area of what happened at Customs, do you think there is evidence of failings at the contract management level in Customs?

**Dr Lewis**—I do not have evidence one way or the other on it.

**Senator LUNDY**—It certainly has been raised in other inquiries. In observations made by the Australian National Audit Office in previous inquiries into IT outsourcing, this very point about the expertise to manage the contracts has been made. The ANAO has reported—and I know Senate committees have had evidence on the fact—that there is a view that the expertise does not exist and that it is one of the unforeseen factors contributing directly to some of the inefficiencies associated with the IT outsourcing process. Is that a fair observation?

**Dr Lewis**—I think it is fair, with the exception of being unforeseen. It was foreseen.

**Senator LUNDY**—That is right; I concede that point.

**Dr Lewis**—Suggestions were made that something should be done about the appropriate education and training of contract managers and the appropriate responsibilities above the contract manager as well, of course. So this is an issue that starts with the CEO and the Financial Management and Accountability Act. The concerns about contract management have certainly been around for a long time, not just in ICT but perhaps particularly so.

**Senator LUNDY**—Thank you. On the overall issue of the security of Commonwealth information and data, what can you see as the necessary action now required, given the breach that occurred at Customs? I know you are not privy to it, but the documents we have just tabled show that, clearly, there are ongoing major problems and issues within agencies and departments.

**Dr Lewis**—That is certainly a very visible symptom of some of the difficulties. There are other more widespread issues with data integrity and so on that need to be looked at. The first action I would take—and this is not necessarily selling the work of Standards Australia—is the implementation of the governance of the information and communication technology standard when it is released. The standard shows that the responsibility for these things in commercial firms is with the board of directors and for the public sector it is with the CEO. Those responsibilities need to be accepted and followed through by the people at that level. The standard then goes on to suggest various ways by which that aspect of governance is carried out.

In all the models of enterprise security architecture that have been developed to now, the starting point is governance—it is the involvement of senior management and the commitment of senior management to security over their information. The acknowledgment of that responsibility and the reflection of that responsibility is in making sure that the appropriate budgets are in place, that the appropriate training is in place and that the appropriate processes and practices are in place.

**Senator LUNDY**—In its report entitled *Implementation of whole-of-government information technology infrastructure consolidation and outsourcing initiative*, the Audit Office found in some cases that the security issues were not resolved in the original contracts and that they were

negotiated subsequently. The Audit Office made recommendations that the gaps in security needed to be addressed. Are you aware of the current practices in relation to security in government contracts and whether agencies and departments, and indeed the government, have actually learnt from some of these previous rather adverse findings by the ANAO?

**Dr Lewis**—I cannot give specific examples because I have not been dealing with specific contracts for a while.

**Senator LUNDY**—I appreciate that, but I think your general observations would be useful.

**Dr Lewis**—Judging from symptoms in other agencies in other areas, I would say no, I do not think that security issues have been addressed as much as they need to be, or data integrity or data insurance as a whole—it is not just the physical protection of assets that is of concern.

**CHAIRMAN**—Laptops seem to be the most vulnerable of the physical assets that we are talking about—and that is all the evidence that we have received so far. What can we do to make them more secure?

**Dr Lewis**—There are a number of practices, and some agencies are following these practices. One is the simple aspect of locking them down—using cables, keys and so on—to make sure that they do not wander out of the building. Overseas evidence indicates that most losses are from the building of the organisation. Some are lost in taxis, some are lost at home, but most seem to be lost from within the building. If there is at least some extra level of protection beyond keys on doors, then that can slow things up. There are alarms and screamers that can be used to make sure that, when a laptop starts to walk, people know about it. There are actions at that level.

There are other issues with laptops, which indicate that, for example, senior executive service people who take them home need to make sure that they are appropriately protected at home. In my view, you should not take a work laptop home and you should not take a home laptop to work, because it leads to other problems like the introduction of viruses into networks. Certainly a major problem facing a lot of agencies at the moment is the fact that people who are issued laptops find it very hard to carry out the normal security arrangements around a laptop—not only protection from loss but protection from viruses and the electronic difficulties that come with them, because they do not have the firewalls or other support with a laptop at home. In general, there are a number of steps that can be taken: physical protection, education in the care and handling of a laptop, appropriate reward and sanction arrangements to encourage people to carry out the policies. Most policies, if they are not well known and if they are not policed, might as well not exist.

**CHAIRMAN**—You said that you think it would be more appropriate if people left their work laptops at work and did not take them home. If we bring that in as a policy, isn't it sort of like giving in to the terrorists? Haven't we given up and given in to the thieves so we should not have a free and open society?

**Dr Lewis**—The loss of laptops through a criminal action is certainly serious. The loss of information or the mistakes that are made through the misuse of laptops is perhaps equally damaging to the efficiency, if not the effectiveness, of the organisation. That is through, say,

misuse of the laptop and the mistakes that are made—deletion of data or the introduction of viruses. So I would say no; I think that the introduction of sound policy is just good housekeeping. It is not a matter of saying to people, 'We have given up.' This is just making sure that an asset is used properly.

**CHAIRMAN**—I thought that one of the advantages of laptops is that they are portable, and most of us use ours as portables. You are proposing that they no longer be portable.

**Mr Smith**—No, you can certainly still take them from place to place. I am just saying that it is dangerous to take a work laptop home and then bring it from home and put it back into the network that you brought it from. You need a separation. Some organisations go through a process, so that when the laptop comes back to the organisation it goes through a cleansing process which checks that there is nothing wrong with the laptop, that it is up to date with its software and so on. Then that laptop is given back to the person to reconnect to the network. There are other practices like that which can provide the appropriate checks and balances around these sorts of risks. It is a matter of risk management. It is a decision that the CEO has to make about how laptops will be used—what benefits there are from the use of the laptop against what dangers there are. It has to be a well-informed risk management exercise.

**Ms GRIERSON**—Just one more question: we asked Commonwealth departments about their incidents, and they have recorded those for us. We have not, unfortunately, had much time to look at them. One incident is contamination of a web site, where pages have been replaced with other pages. Can you explain how easy or difficult that is, and how difficult or easy it is to prevent that happening?

**Dr Lewis**—It is often and easily done, and it is often and easily protected against.

**Ms GRIERSON**—So you would assume that all Commonwealth departments could easily protect themselves against any of their web site information being replaced with inaccurate information?

**Dr Lewis**—Yes.

**Ms GRIERSON**—We will have to see if it comes up again.

**Ms KING**—I think you would have heard the previous witness say that he thought that IT outsourcing had in fact improved IT security. Do you agree with that?

**Dr Lewis**—Not necessarily—reflecting back on the previous answer I gave in the sense that, even with a good contract, if you do not have good contract management then the risks continue. Certainly the need to raise a contract and to go through the evaluation of vendors has made visible a lot of IT management issues that were normally taken for granted. In that regard, it has certainly raised the awareness of some of these sorts of things but the risks have not necessarily gone away.

**Ms KING**—And it has brought forward a whole new set of problems.

**CHAIRMAN**—Dr Lewis, I would think that we are giving publicity to these issues far and above what anyone else has done before. Thank you for coming. If we have further questions, would you mind if we put them in writing?

**Dr Lewis**—No, I would be delighted.

**CHAIRMAN**—Thank you.

[10.07 a.m.]

**NOCKELS, Mr James Alexander, First Assistant Director-General Security, Australian Security Intelligence Organisation**

**CHAIRMAN**—I now welcome the representative from the Australian Security Intelligence Organisation appearing at today's public hearing. Thank you very much for coming, and thank you for your brief submission. A number of Commonwealth agencies store computer backup files off site with private companies. Does ASIO see the use of such private sector companies as a weak link in the chain of security integrity of Commonwealth data storage?

**Mr Nockels**—Not if the material is stored appropriately and securely—meeting the necessary and appropriate standards pertaining to that material.

**CHAIRMAN**—Would you believe that storing computer tapes in a wheelie bin was appropriate?

**Mr Nockels**—It would depend on what level of classification the material being stored in the wheelie bin was. As I am sure you are aware, there are levels of protection relating directly to the sensitivity or importance of material. I think most Commonwealth standards and appropriate regulations relate almost directly to the association of the material to its level of security clearance. I do not know what level of clearance, if any, the material in the wheelie bin was. It may have been quite appropriate if that was how they were moving material around—although I would think that most IT people would prefer not to store their tapes in wheelie bins, but that is a matter for professionals to comment on.

**CHAIRMAN**—Do you allow your staff to use laptops?

**Mr Nockels**—In certain controlled and very limited situations.

**CHAIRMAN**—Why is that?

**Mr Nockels**—Because of the importance and integrity of the information which ASIO is responsible for holding. ASIO's information storage and retrieval system is totally isolated and air-gapped from external contact. We have no external connectivity between our domestic computer system and the outside.

Our use of laptops relates to two levels, and there are specific and clear regulations about those. Certain laptops are issued to officers for unclassified work. That would be work that officers are undertaking on behalf of, say, the provision of certain sorts of advice or the gathering of certain sorts of information that is unclassified. There is a second level, where a laptop may need to be used to carry a large amount of classified data to meet a specific requirement—for example, a presentation to the Joint Parliamentary Committee on ASIO, ASIS and DSD. That information would be downloaded from the system onto the laptop. After use, the information would be checked and audited and the laptop, as Dr Lewis talked about earlier, would be appropriately cleansed. We specifically note that any laptop used for classified purposes remains

one that can only be used for classified purposes, because it is obvious that there is still a capacity to gain data from that laptop, whatever anyone has done. We specifically and clearly separate the use of that equipment and it is under extremely complex controls, as it needs to be.

**CHAIRMAN**—You were here when Dr Lewis spoke, so you would have heard him say that it is perhaps more appropriate not to allow laptops to be taken outside of a business environment. The submissions that we have received indicate that a reasonable number of laptops have been stolen or lost from Commonwealth premises, private cars, homes and everywhere else, but there is no indication that there has been any major breach of security as a result of any of those thefts. Do you think it is appropriate for other Commonwealth agencies to use laptops and to allow them to move around as portable devices?

**Mr Nockels**—We are in the information age. I note that Senator Lundy is using her computer. I think there is a reality in the world that says we are more and more turning to electronic information to facilitate the work of government organisations. It would be useful and appropriate in a range of situations for people to use computers, and for that reason I think it is a matter of the chief executive of the organisation making a decision about the utility of computers and how much they assist in the efficiency and productivity of an organisation. The important thing—and I think Dr Lewis talked about this—is that appropriate protections and processes be put in place and that individuals understand the importance and responsibility they carry with them when handling material in any form, whether it be paper or computers. Historically I am sure as much paper has been lost. One can read novels about the important pieces of paper left in the railway carriage going from Victoria Station to somewhere in 1857 or whenever. The realities are that this is always with us. The real issue is that the processes are put in place and individuals are made aware of their responsibilities. I do not think you can be as utopian as to suggest a yes or no solution.

**CHAIRMAN**—You are trying to say: 'Let's keep things in perspective.' I left one camera on a train one day and I left another one in a taxi cab. Leaving cameras lying around is getting very expensive for me, but I do not think national security was every impugned.

**Ms KING**—Is ASIO only called in to investigate incidents where IT security is linked to a breach in national security?

**Mr Nockels**—Yes. It is a national security issue. As I tried to explain in our submission, from time to time we are asked by a number of agencies to provide professional advice, and from time to time we could be asked to provide advice on a specific aspect of something, but our responsibilities relate to investigating, with other authorities as appropriate, breaches of national security in terms of possibly improper use of classified information.

**Ms KING**—We have had three incidents, one of which I suspect is about to hit the media. There was Australian Customs Service, where the two servers disappeared; there was DOTARS with the laptop; and we now have evidence before us that a whole number of backup tapes from group 5 agencies were disposed of in a wheelie bin, which is pretty frightening. Has ASIO been involved in investigating each of those three incidents?

**Mr Nockels**—We normally ask if we are aware of it, or there is a public awareness of it and if they believe there is a national security issue involved. If there is not, we do not become

involved. If there is a national security issue involved, the agency has a responsibility to inform us.

**Ms KING**—Have you been involved with those three incidents?

**Mr Nockels**—No.

**Ms KING**—Not at all?

**Mr Nockels**—Sorry, we have not been involved in investigations. We are aware of them and, in various elements of investigations we may or may not be called to give advice at an appropriate time.

**Ms KING**—They are certainly the three that we know of. Are you involved in any other investigations that you can tell us about?

**Mr Nockels**—No, I am sorry.

**Ms GRIERSON**—I note from replies we have had from Commonwealth departments that the Department of the Prime Minister and Cabinet have had laptops stolen. But they say that all their information on laptops is encrypted. Are you aware of which agencies have absolute encryption of all their information?

**Mr Nockels**—I am not sure that any have absolute encryption.

**Ms KING**—What does that mean?

**Ms GRIERSON**—Except PM&C perhaps?

**Mr Nockels**—I cannot comment. Certainly there are levels of encryption and means of providing a very significant level of protection to data on computers. But, in most cases, where there is a will, there is a way and, with sufficient time and energy, these things can be decrypted.

**Ms GRIERSON**—Part of the reason for reopening this inquiry and obviously our aviation security inquiry was the atmosphere and the concerns regarding terrorism. One would think controlling who comes into this country would be a major aim—and one that you would be very interested in. Would you be aware of whether Customs and Immigration have encryption software on their computers?

**Mr Nockels**—That would be a matter that does not fall within our purview.

**Ms GRIERSON**—You are an adviser to government.

**Mr Nockels**—On physical security, not IT security.

**Ms GRIERSON**—So you do not advise on those sorts of levels?

**Mr Nockels**—No, DSD are the national authority on those matters.

**Ms GRIERSON**—We will ask those questions of DSD this afternoon.

**Mr Nockels**—As I tried to explain in our submission, we are responsible for the physical parameters of the environment in which an IT system or computer related equipment is stored.

**Ms GRIERSON**—Within that responsibility, have you made recommendations to Customs in relation to the incident that they had?

**Mr Nockels**—Not in relation to that specific incident, although we have undertaken, and do undertake, work on a range of issues for Customs. With regard to the particular incident which I have seen reported in the press; that is, the loss of, I think, a laptop and a bottle of whisky—

**Ms GRIERSON**—No, it was the loss of two servers. That was the DOTARS incident.

**Mr Nockels**—With regard to Customs, not in relation to that specific building.

**Senator LUNDY**—I would like to go to the issue of the wheelie bin disposal of tapes from group 5 agencies and departments. In response to questions from the chairman to the Department of the Prime Minister and Cabinet—and, indeed, I think the same statement is in the Department of Transport and Regional Services and Department of Communications, Information Technology and the Arts responses—the answer was that ASIO were informed immediately of the incident once Telstra became aware of it. What is precisely your role on being informed of such an incident?

**Mr Nockels**—We make an assessment—and this is usually done in association with the Australian Federal Police, recalling our role is an advisory one—of whether the incident is likely to have involved, in a generic sense, espionage or, in other words, the attempt to gain this material by individuals or agencies whose interests are inimical to those of Australia. On the basis of that assessment we then decide whether or not to become involved in an investigation. In the case of this one—the Telstra data—a judgment was made that, at that time, it did not appear to be an issue that related to our responsibilities in that regard.

**Senator LUNDY**—You made an assessment that you did not think espionage was involved.

**Mr Nockels**—That is correct. I believe, and the last I understood, is that investigations are continuing. If anything emerges from those investigations that suggests otherwise, we can of course become re-engaged.

**Senator LUNDY**—Going a little further on that, these reports state that the tapes were never recovered. We are talking about backup tapes from PM&C, DCITA, DOTARS et cetera that were never recovered. How were you able to make a determination that espionage was not involved if those tapes were not recovered?

**Mr Nockels**—Partly due to advice as to the type of material that was being backed up and, secondly, the potential utility of that material to someone else.

**Senator LUNDY**—Was it encrypted?

**Mr Nockels**—I do not believe it was encrypted.

**Senator LUNDY**—But you made an assessment that it would not be of much use.

**Mr Nockels**—And also because of the environment in which the incident occurred. Obviously I am not able to fully advise you on the detail of the investigations, but the general parameters of what occurred suggested that there was a stronger likelihood that it was an administrative error and sloppy handling of the material rather than any suggestion that someone from the outside got into the computer area and in some way physically removed them. That, linked with our understanding of what was on the tapes, suggested that it was unlikely to be a target of the sort we would be concerned about and more likely to be a matter that required a police investigation—more particularly, an investigation of process and procedure, which I believe is ongoing.

**Senator LUNDY**—Can you confirm that the backup tapes were kept in the wheelie bin and the implication of the answers to questions we have received that they were accidentally disposed of as rubbish? That is the speculation contained in this report.

**Mr Nockels**—That is the speculation, and I would emphasise that that is just what it is: it is speculation until a proper and thorough report is delivered.

**Senator LUNDY**—Are you aware of any other security incidents or incidents within the affected departments under the group 5 contract that Telstra services—perhaps a server failure—that could be related to the disappearance of the backup tapes? Are you aware of corresponding technical problems, not necessarily involving security breaches, that occurred at the same time that the backup tapes disappeared?

**Mr Nockels**—I honestly could not comment on that. That really is a matter for IT experts to comment on.

**Senator LUNDY**—Who would be the investigating authority to look at those related matters?

**Mr Nockels**—If it relates to the IT system itself, to the software and the hardware, that falls clearly with Defence Signals Directorate IT security people, as I am sure you aware, who have Commonwealth responsibility for setting standards and undertaking appropriate investigations if necessary. We obviously work with them because sometimes it is not clear whether it is a physical perimeter point of view, a personnel security point of view or an IT system point of view. Because they require different levels of expertise, those responsibilities lie with different agencies.

**Senator LUNDY**—Do you think that the complexity of where responsibility lies is one of the real challenges related to security? Some of it is with DSD and some of it is with the agencies themselves, and NOIE sticks their head up from time to time saying, 'We're coordinating it all'—they are obviously not doing a very good job. I think Telstra Enterprise Services provides their IT services too.

**Mr Nockels**—I think we are moving into a complex world. I do not think we all fully understand it yet. I certainly think there will always be room for improving our approaches. Historically, for very sound and sensible reasons, DSD has carried IT security. For similar reasons, our organisation has provided the physical security advice. We work very closely and are in regular discussion on a range of issues, and I think the various publications note that there is a duality of responsibility. It is no good having an IT system being certified as approved, with high levels of encryption and everything else, if anybody can walk in and out of the door or if staff whom you have no confidence in can gain access. We have covered that physical security and provided, where it is appropriate, top-secret, positive-vetting comments on individuals. DSD does the IT security. The bulk of data being handled by Commonwealth departments certainly does not fall into the national security classification category but is, if I can put it this way, the 'grist of government'; therefore, the need for the application of security processes and procedures really has to lie with the chief executives of those organisations to make the decision as to where they feel their data needs to be protected, for whatever reasons.

**Senator LUNDY**—Given that PM&C handle extremely sensitive and cabinet-in-confidence information, that implies that it would be at the highest level of security. Are you able to tell the committee the security status of the backup tapes that were in a wheelie bin?

**Mr Nockels**—No, I cannot. The facility that the event occurred in was an appropriately accredited facility. What I am suggesting is that the event seems to have occurred within, rather than there being a breach of, the physical security parameters—just as the Department of the Prime Minister and Cabinet handles classified material but not all of the Department of the Prime Minister and Cabinet's material is classified. Those areas that do handle top-secret material are accredited by us and are appropriately compartmentalised in terms of their IT systems and their physical security.

**CHAIRMAN**—When you were talking about your relationship with, particularly, the AFP and with other government agencies, is any of this in writing? I do not mean to imply that there is anything negative in that, but have we developed an ad hoc arrangement in this regard?

**Mr Nockels**—No. With regard to the investigation of potential breaches of national classified information, there are clear standards and processes for that. On a few occasions those have been reinforced, not least by, for example, formal advice from the Prime Minister to ministers and agencies as to the reporting and investigation of potential breaches of national security.

**CHAIRMAN**—This committee has, from time to time, shown a great liking for memoranda of understanding. It is our belief that they are extremely useful. Have you ever considered that route?

**Mr Nockels**—I think that usually, when systems are operating well and under clear direction, it is possibly unnecessary. One might want to consider that if systems are not working. Across the issue of handling potential breaches of national security, the relationship between ourselves and the AFP is very much hand in glove. I would re-emphasise our advisory role; the formal and detailed investigation and the capacity to prosecute obviously lies with the police, and so there is a logical train of activity that takes you to that—

**CHAIRMAN**—That all sounds logical, but you did say that this is an evolving scenario.

**Mr Nockels**—Sorry—I was referring to the use of IT, not the investigation of breaches of national security.

**CHAIRMAN**—I understand that, but because technology keeps moving on, and because security issues keep changing—you would be aware that we are conducting a dual inquiry into aviation security at the moment, which involves ASIO very much—I just wonder whether, as the scenarios evolve and as times change, a more formal relationship might be useful. For instance, in the Coastwatch inquiry we found with the relationship between Customs and other agencies, including the AFP and the Department of Defence, those formal documents were a great deal of assistance and have allowed that national command centre to operate in a very much more enlightened and time responsive manner.

**Mr Nockels**—As I said, Mr Chairman, processes are working well as far as I am concerned. We have not seen any need for anything to be enshrined. I reiterate: there are already clear, established procedures for handling breaches of national security. I certainly have not looked at them and asked myself whether they would be better formulated in a memorandum of understanding rather than having established administrative procedures.

**CHAIRMAN**—Would you like to think about that and come back and give us your views—or is that asking a bit much?

**Mr Nockels**—I would simply reiterate that the processes are working well as they are. As to the suggestion that we undertake investigations of a memorandum of understanding, against quite a busy workload at the moment—I cannot say that it would be nugatory—it would be questionable at this stage.

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

**Mr Nockels**—Not at all.

**CHAIRMAN**—Thank you very much. Is it the wish of the committee that the Attorney-General's response be authorised for publication? There being no objection, it is so ordered.

**Proceedings suspended from 10.31 a.m. to 10.43 a.m.**

**BANHAM, Mr David, Chief Information Officer, Department of Transport and Regional Services**

**FISHER, Mr Robert, First Assistant Secretary, Corporate, Department of Transport and Regional Services**

**TONGUE, Mr Andrew, First Assistant Secretary, Transport Security Regulation, Department of Transport and Regional Services**

**YUILE, Mr Peter, Deputy Secretary, Department of Transport and Regional Services**

**CHAIRMAN**—Thank you, gentlemen, for coming. I thank the Acting Deputy Secretary for his letter. The first thing I want to say is that, while we were disappointed to read in the *Herald Sun* about the theft of a laptop at DOTARS, I do want to thank the department for immediately telephoning me and apologising for not realising that the two inquiries were ongoing and related and for then following it up with essentially a letter of apology. I cannot speak for my colleagues but I thought that was appropriate, and I appreciate it very much. Could you tell us whether or not you keep any of your backup material off site and, if so, how you secure it?

**Mr Yuile**—Our IT is managed by Telstra Enterprise Services. They have the responsibility for backup and storage of our material, our IT system and our email service. They are stored off site by them. I should ask David Banham, who is our chief information officer.

**Mr Banham**—As a general rule, a large number of our corporate systems are off site, on TES property. The daily backups would not as a rule be stored off site. The monthly backups are stored off site in secure storage.

**CHAIRMAN**—You used the two words 'secure storage'. Is DOTARS happy with the security arrangements off site or, for that matter, on site?

**Mr Banham**—As a general rule, yes we are satisfied. We had a recent audit done of the services provided by TES. You would be aware of a recent incident where there was a breakdown in procedures.

**CHAIRMAN**—I certainly am.

**Mr Banham**—Apart from that incident, we are comfortable that the secure off-site storage is appropriate for our requirements.

**Senator LUNDY**—Do they still keep it in the wheelie bin?

**Mr Banham**—No.

**CHAIRMAN**—Although it was convenient, it did not work very well, did it! Are you still convinced that that was an accident or procedural breakdown—that is, you suspect that a cleaner

took a wheelie bin and dumped it in the rubbish? Do you still have ongoing concerns that the backup tapes might someday be used for some nefarious purpose?

**Mr Yuile**—That is obviously a difficult question. What I can say is that clearly it was a major breakdown and one which the service provider has acknowledged as serious. They have intervened at the highest levels to reappraise and strengthen their procedures and their processes. Included in that, as I understand it, is regular auditing. The group 5 departments also have instituted random auditing. All the information that we have to date indicates that there was not any criminal intent and that the material has not been accessed and used, but we will keep that under careful monitoring.

**CHAIRMAN**—The information would not compromise national security if it were to be used?

**Mr Yuile**—Our policy is that only material up to a protected level is on our system, and that does not include national security material.

**CHAIRMAN**—You gave us details of the laptop. Others have been stolen or lost or have disappeared. Are there better procedures we could put in place to better protect portable computers?

**Mr Yuile**—Maybe others who are better experienced than me could answer that. I would say that four over the period of time is not desirable but is probably not a bad record. I do not know what the records are in other departments, or indeed in Parliament House, but it is a portable computer and by their very nature they are easily stolen and easily mislaid. We endeavour to take all the steps we can to impress upon staff the need to secure these when they are travelling and not to have any material that is of a sensitive or highly classified nature. There are operational requirements. We have safety investigators who go out into the field and have to regularly transmit material back to Canberra and get quick reports back. We impress upon them the need to take due care and responsibility for that equipment. I am not sure what more we could do. If we withdraw them from people, we run into operational difficulties with the nature of business.

**Mr Fisher**—To put it in context, DOTARS has lost four in four years. For a department of 1,000 people, it is better than a lot of departments. With a department of 1,000 people, one laptop out of 1,000 people a year is not good. The laptops belong to Telstra, not to DOTARS. We have not lost Commonwealth property. We would like to lose none. In one circumstance, there was a break-in at an officer's home, where they lost a lot of personal and other belongings. The laptop went as well. There is not a lot the department can do to prevent active criminality.

**CHAIRMAN**—Dr Lewis suggested this morning, when you were not here, that perhaps they should be locked down in offices. That is in both the private sector as well as the public sector. How would that appeal to you?

**Mr Fisher**—Without challenging Dr Lewis's authority, the question for me is that it is not a very mobile bit of equipment if it is locked in an office 24/7.

**Ms KING**—Are you saying only four laptops have been lost or stolen from the department?

**Mr Yuile**—Since 1998.

**Ms KING**—The last was 22 August?

**Mr Yuile**—Yes.

**Ms KING**—The information that came out through the media and that you gave to us was that the laptop contained briefing information and a PowerPoint presentation and, in your assessment, it was not national security information. What else was contained on the laptop?

**Mr Yuile**—I will invite Andrew Tongue to respond to that as it was from his area.

**Mr Tongue**—The laptop was used in a docking station arrangement, where it plugs in on the officer's desk and then is used to access all the normal desktop services of the department. In that instance it is pathing through to the system maintained by TES; it is not actually resident on the laptop.

**Ms KING**—So the officer does not use the C drive on the laptop to store any information at all other than a PowerPoint presentation?

**Mr Tongue**—That is right. The laptop had been used and carted around Australia for a series of workshops with industry.

**Ms KING**—Who runs those workshops?

**Mr Tongue**—A number of my staff.

**Ms KING**—So it was one of your staff's computers?

**Mr Tongue**—Yes.

**Mr Yuile**—No, it was the department's computer that he was using. A test computer—

**Ms KING**—Was it your computer that you were using?

**Mr Tongue**—No, it was the computer allocated to him.

**Ms KING**—What level was that person?

**Mr Tongue**—An EL1. The laptop had on it a presentation that we were using as part of the implementation of new maritime security arrangements. It was used to conduct workshops around Australia that involved 700 or 750 people. It was a standard presentation that we were using to, if you like, kick off the workshops.

**Ms KING**—When he goes into work at DOTARS, is that the only computer that he has on his desk—a docking station?

**Mr Tongue**—Yes, that is right.

**Ms KING**—To be quite honest, having worked in departments, I do find it somewhat hard to believe that that would have been the only document sitting on that laptop. I find that quite unusual.

**Mr Banham**—Our laptop computers are configured with a product called Citrix, which basically means that they access the services on our servers rather than the services locally on the computer itself.

**Ms KING**—Being a bit slack about filing things every now and again, I store lots of documents on my desktop—lots of them. So it is not unusual to find lots on your desktop or lots on your C drive. I do not know that many people—other than probably Kate—who are that disciplined.

**Senator LUNDY**—I have a lot on my C drive too.

**Ms KING**—You have lots as well. So I find that quite unusual. Where was the breakdown in security?

**Mr Yuile**—In what sense?

**Ms KING**—How did it go?

**Mr Yuile**—Do you mean the break-in?

**Ms KING**—Where was the breakdown in security? Obviously there has been a breakdown in security for a laptop to be stolen. Where do you think the breakdown was?

**Mr Yuile**—In this instance, there was an unauthorised entry into our building.

**Ms KING**—But how did that happen?

**Mr Fisher**—I am not sure that I would describe it as a breakdown. Somebody physically broke into the building.

**Ms KING**—How did they get in?

**Mr Fisher**—They took a card.

**Ms KING**—When did they take that card?

**Mr Fisher**—I do not know. They took a card that was not issued by the department—it was not the department's card.

**Ms KING**—I understand it was from the cleaning staff. Do you know when that card first disappeared?

**Mr Fisher**—No, I do not. The cleaner reported the card missing.

**Ms KING**—Does anyone in the department know when the card went missing?

**Mr Fisher**—I do not think that the department could possibly answer that. If we knew when it went missing we would be able to apprehend the thief. We know when the card was reported missing, but we do not know when it was taken.

**Ms KING**—When was it reported missing?

**Mr Banham**—It was actually reported missing after the event itself. Based on when the cleaner involved was last aware that they saw the card, the best we could ascertain was that the card disappeared probably within a 24-hour or 48-hour period before the incident.

**Mr Fisher**—There is a public perception that somebody wandered into the department, picked up a laptop and wandered away. The fact is that there was use of a card to access the building.

**Ms KING**—I would call that a breakdown in security.

**Mr Fisher**—This is a public building with public access, and the card that was stolen provided access to common use public access parts of the building. There is another wall behind which the department's assets are located, and that was physically broken into. It was a criminal act. A physical break-in is an act of criminality. This is not the department in some way being slack and leaving doors open. We can take measures to protect against acts of criminality but we cannot stop them.

**Ms KING**—I guess you can also take measures against things that happen in the lives of lots of people: they misplace their security passes; cleaning staff, which the department has a contract with, might misplace or lose their security passes.

**Mr Fisher**—I would just like to correct that. This was not a cleaner that the department had a contract with. This was a cleaning firm that the owner of the building had a contract with. The department is one of a number of tenants of the building. The cleaning firm concerned did not have access to the department's part of the premises, so there is not any direct relationship between the department and the cleaning contractor.

**Ms KING**—Was it very hard for them to get in? Obviously they have used the security pass to enter the building, and you have said that they then broke into the DOTARS area. How hard was that to do? From the timing that you have talked about, it does not appear to have taken them a lengthy period to get in there.

**Mr Yuile**—They had to smash glass doors to get through.

**Ms KING**—Yes, a few seconds?

**Mr Yuile**—I have no idea.

**Ms KING**—I do not know; I was just asking the question.

**Senator LUNDY**—On the issue of the security event when the laptop was stolen, were other laptops in the vicinity? Why was that one targeted?

**Mr Yuile**—Other things were taken from other areas of the building.

**Mr Tongue**—I think that was the only docking station in the immediate vicinity. Immediately around it there were standard desktop configurations with the big boxes. But, at that time, in that immediate area it would have been one of the few docking stations.

**Senator LUNDY**—So you should be able to tell me now whether there were any other laptops physically in the vicinity.

**Mr Tongue**—I do not believe there were, but I would need to check to make sure that I am dead right.

**Ms KING**—Do you have a classification of levels of people who have access to laptops? Or is it that, if staff request it, they can have a laptop with a docking station instead of a PC?

**Mr Tongue**—It depends a bit on their need. The advantage of docking stations is that it saves us money. We buy one computer rather than having a box on the desk and all that. It depends a bit on need rather than on the levels.

**Ms KING**—Is it common for junior staff to have laptops?

**Mr Fisher**—What do you mean by common? We do not use laptops in the way that MPs use laptops. I do not know how you compare or how you make a judgment as to what is common and what is not.

**Ms KING**—Does everybody have one?

**Mr Fisher**—No. We have fewer than MPs have. We have fewer than some departments and probably more than others. Everybody does not get issued with one as a matter of course. If people need one for work purposes, they get access to one.

**Ms KING**—They have to specifically request one?

**Mr Fisher**—That is exactly right.

**Mr Yuile**—It is a supervisor's decision about operational need, and it is a sensible arrangement.

**Ms GRIERSON**—Do you think that the laptop taken was randomly selected, given that they have obviously attempted it on other floors or in other areas? Do you have any view on that?

**Mr Fisher**—It is hard to judge. The other items that went missing were a LitePro projector, a $20 bottle of whisky and some petty cash.

**CHAIRMAN**—That is pretty cheap whisky.

**Mr Tongue**—It was a gift to a staff member who had left a work area and joined our work area, and they stored it at work. We were not sitting around having a tipple.

**Ms KING**—No, I was not questioning that.

**CHAIRMAN**—Not at $20 a bottle.

**Mr Fisher**—Given the items that went missing, it does not sound like a highly targeted operation.

**Ms GRIERSON**—Was that area in DOTARS easier to access than other areas? Were the door systems any different or was the glass that was smashed any different?

**Mr Banham**—They tried a number of areas. You can see where they tried getting in with a pass, which was unsuccessful because our system is independent from the building system. I understand that the laptop was taken from the second place. They broke one set of doors by breaking the fire alarm to free up the doors. So the laptop computer would have been taken from the second place they visited.

**Mr Yuile**—We cannot speculate.

**Ms GRIERSON**—But you will speculate; it is very important to speculate.

**Mr Yuile**—All the evidence suggests that it was opportunistic.

**Ms GRIERSON**—Have you changed any procedures regarding the lost pass—such as access to the building or tightening levels of access in some way?

**Mr Fisher**—The lost pass was not our problem, in that the lost pass provided no access whatever to the DOTARS secure area. The lost pass was access to a public common use area shared with other tenants, including the coffee shop. The access to the DOTARS secure area was a physical break-in at the second barrier point. In response to that, we have also put in place a 24-hour guard who wanders the floor just to make sure that there are no opportunistic break-ins of our secure area.

**Ms GRIERSON**—Is that a permanent response?

**Mr Yuile**—We have taken that immediate step, and we are having a further risk assessment on the building, and our security committee and our property area are reviewing whether that is the best long-term solution or whether there might be other solutions. So we are actively looking at how to harden positions.

**Ms GRIERSON**—Have you issued staff with guidelines about what should be retained on laptops and what should not?

**Mr Yuile**—Yes, we have. We have standing instructions in terms of our IT and security, and that has been further upgraded recently with the issuing of new policy.

**Mr Banham**—That is correct.

**Ms GRIERSON**—I assume your system is very much like ours. When we put our laptops into our docking stations we then have access to the whole server system. It is just a password that gets me in, basically. How difficult is it to breach that system?

**Mr Banham**—The moment we discovered the laptop was missing, the service provider was informed and the access of that machine was disabled. So, even if they did have the userid and password associated with that laptop, it was automatically disabled.

**Ms GRIERSON**—What was the timing process for that?

**Mr Fisher**—If I could add: there is no evidence that anybody had access to the personal password or that the password was used at the time of the theft.

**Mr Banham**—It would have been done within 30 minutes of discovering the theft.

**Senator LUNDY**—In the area the laptop was taken from, can you tell me whether there were any attempts to break into any filing cabinets? And could you itemise what else was taken in that incident—both from that area and other areas?

**Mr Fisher**—The only items that we are aware of that were missing on the night were the laptop, a LitePro projector, a $20 bottle of whiskey and some petty cash. We found the LitePro projector discarded in another work area. We never found the bottle of whiskey, the petty cash or the laptop.

**Senator LUNDY**—Were any filing cabinets or desks broken into?

**Mr Fisher**—There was no evidence that they had been broken into, and no staff reported any other items missing or tampered with.

**Senator LUNDY**—I know that you covered this in previous questions, but can you tell me whether or not the department has implemented a clean desk policy since the breakdown—that is, no-one can leave any stuff around at all?

**Mr Fisher**—No, the department has not got a clean desk policy. I guess we need to recognise the nature of the department. It is diverse; it has a range of different functions. Some of them have security implications, and some of them go to providing services to the public and other services. The department does not have a clean desk policy, but the transport security area has its own particular arrangements. I invite Mr Tongue to talk to the arrangements in that work area.

**Mr Yuile**—Just before he does, I would like to make a point. Different people use the term ‘clean desk’. Some people mean that there is not a scrap of paper on the desk and other people mean that classified and sensitive information is not on the desk—that it is appropriately secured but other things are on the desk. Some of us started in departments where you left nothing on the

desk at the end of the day. It did not mean that things were properly secured, I have to say. So I think the definition is important in that instance. We do have very clear guidelines about people securing classified and sensitive information. Depending on the levels of that information, we have a layered set of secure arrangements.

**Senator LUNDY**—Were they in place before the break-in?

**Mr Yuile**—Yes.

**Senator LUNDY**—So you have not changed that arrangement since the break-in?

**Mr Yuile**—We are again looking at all of our arrangements to check those, but we certainly had them within our instructions.

**Mr Tongue**—Because we handle some national security classified information, we have a range of storage arrangements that you would not find in the rest of the department—B-class containers, B-class filing cabinets—in a secure area in a completely different part of the department that is separately alarmed and so on. We handle all of the national security classified information in accordance with various requirements.

In addition to the measures that have been described, because of the profile that the issue raised, I have taken separate steps with my staff to put in place some additional arrangements around the handling of laptop computers around home based work and that sort of thing, simply because I was concerned that we might get somebody who might seek to make a point by having another crack at us. So we have put in place some additional things.

**Mr Yuile**—I brought my laptop in because I did not want to risk a home break-in.

**Mr Tongue**—We have spoken further to ASIO and we will be undertaking some additional work.

**Ms KING**—With the 22 August and February 2003 laptops, clearly you notified the AFP about the latter one, but I am not sure about the prior incident. Were ASIO or DSD notified either by your department or by the AFP?

**Mr Yuile**—Certainly the AFP would have been notified.

**Mr Banham**—I can tell you that the last one was notified to DSD.

**Ms KING**—Why?

**Mr Banham**—Unless it involved a security incident, we probably would not talk to DSD about it but, because it became fairly high profile, we talked to DSD and put in a—

**CHAIRMAN**—It did become fairly high profile, didn't it?

**Ms GRIERSON**—Was there encryption software loaded onto that laptop?

**Mr Banham**—No, there was not. We do not consider that laptop to be a security issue. We alerted DSD after a conversation with DSD about the issue. They saw it in the newspaper, they talked to us and we gave them the information.

**Ms KING**—So DSD were worried about national security issues in relation to the laptop?

**Mr Banham**—No.

**Ms KING**—DSD do not generally get involved with laptop theft investigations at departments, from what I have gathered.

**Mr Banham**—They have not got involved. Rather than explain it on the phone, we simply put the facts down on a piece of paper and gave it to them for their records.

**Mr Yuile**—The way it was reported, it would have been reasonable for them to ask the question, but the report was incorrect.

**Ms KING**—Has the AFP inquiry into the laptop theft been completed?

**Mr Yuile**—You would have to talk to the AFP.

**Mr Fisher**—It is in the AFP's hands. As far as we are concerned—

**Ms KING**—Have they reported back to you?

**Mr Fisher**—This was an opportunistic theft of somebody else's material. There was no departmental asset missing. We found the LitePro. The AFP were called in, and they have done the usual, thorough AFP job.

**Ms KING**—Which as yet they have not completed.

**Mr Fisher**—You would have to talk to the AFP. I am not in a position to talk about AFP inquiries.

**Senator LUNDY**—I want to also ask some questions about that other break-in. Can you tell me whether any other break-ins have occurred in the same physical location as the incident we have been discussing?

**Mr Fisher**—Sorry, Senator—which other break-in?

**Senator LUNDY**—The break-in we have just been discussing—22 August. Had there been any other break-ins into that physical location?

**Mr Yuile**—Not that have been reported to us.

**Senator LUNDY**—Has anything been stolen that would normally have been located in that physical location—for example, the laptop stolen from the house earlier in the year?

**Mr Fisher**—It is a broad question. My understanding is that some years ago some equipment went missing from that area when it was occupied by another part of the department, before the transport security area existed.

**Mr Yuile**—Just to add to that: my recollection—and it is a recollection—is not that it was a break-in but that there might have been some theft internally. As Mr Fisher said, it was not the same workgroup that occupied that area and there was no security information.

**Senator LUNDY**—Going back to the question about the laptop that was stolen from the private residence in February, was that staff member based in the same physical area as where the break-in occurred in August?

**Mr Tongue**—Yes, in an office adjacent to that open area.

**Senator LUNDY**—Can you confirm personally that there was no way that the laptop that was stolen from a private residence in February 2003 could have been stolen from the workplace? Are you able to confirm that it was stolen from the house?

**Mr Tongue**—It was stolen along with a range of personal belongings of the officer. The break-in was reported to the police, and the laptop was listed as part of the items. It was reported to the department in the appropriate way. I understand that there was a police investigation. My understanding is that a large television set was stolen. Stereo equipment, kids' videotapes and a whole range of things went.

**Mr Yuile**—The implication of your question is that the answer we gave you in writing was not true. I certainly reject that.

**Senator LUNDY**—We have established one thing. There is obviously some information in the public arena and claims that there was another theft from that area, from the department. That is my understanding.

**Mr Yuile**—There was a theft from a home.

**Senator LUNDY**—I am just trying to find out whether there is any link between that theft from the home and the vulnerabilities at the physical location of the department. All we have established so far is that the employee was also in Mr Tongue's area. If they had been at work with the laptop, it would have been physically located in that area. I am not implying anything other than establishing that fact.

**Mr Yuile**—I do not know the answer to that question. Did you have a look at the docking station?

**Mr Tongue**—No. That particular officer does not have a docking station. The officer was using one of our pool laptops, which is available for people to go through the same system of plugging it in, logging into Citrix and scoring the information in the central system. I would have to talk to him about what he was working on. I think he was working on some draft guidance material that he was sending out to the maritime sector.

**Ms GRIERSON**—He did not have the regulations for the bill, did he?

**Mr Tongue**—No.

**Ms GRIERSON**—What a pity! We'd like to see those too.

**Ms KING**—Do all officers in your area have remote access?

**Mr Tongue**—Remote access is something that people apply for, and we make a judgment about whether they need it.

**Senator LUNDY**—Can you tell us whether the laptop that was stolen from home had remote access and what that laptop was being used for at the time?

**Mr Tongue**—It had remote access. I would have to talk to the officer to ascertain from him exactly what he was working on, but around that time he was preparing the guidance material that we were putting out to these workshops that I talked about.

**Mr Fisher**—Can we just clarify that? I think there might be misleading inferences taken from what Mr Tongue said, although what he said was correct. As you would know, Senator Lundy, there are steps in providing remote access. One is to configure the laptop so that it is physically capable of connecting to the network and the other is to authorise the officer via passwords and so on so the laptop can actually be used to access. I want to clarify a mistaken apprehension that simply by plugging in the laptop you get instant access to the DOTARS network. You do not. There is no evidence that, after the theft, that laptop was used to access the DOTARS network.

**Ms GRIERSON**—With remote access, is there a specific classification of staff member who can use remote access? If they do have that access, are there levels of access, or do they get the whole system?

**Mr Fisher**—That is a good question but it has a fairly complicated answer. The short answer is: no, there is no classification level.

**Ms GRIERSON**—So it is on an individual allocation to an individual staff member at the discretion of some sort of senior officer?

**Mr Fisher**—That is right. Individual officers have access to different parts of the network, depending on where they work and their—

**Ms GRIERSON**—Would you be able to provide us with an overview of your access, the levels that exist and any barriers that are built into it?

**Mr Yuile**—Can I do that now?

**Ms GRIERSON**—No, I am happy for you to take it on notice to provide that.

**Ms KING**—In relation to the laptop theft from home, it seems somewhat of a coincidence that it was almost the same material that seems to have gone missing twice on the same laptops. Is it right that it is not the same material?

**Mr Tongue**—No. Simply by reason of circumstance with the team involved in the preparation of this maritime work, something happened at somebody's home and something happened at work. I do not know what the statistical probabilities are but that was all it was. At the time, because of where we are on this maritime thing—preparation of new legislation, the preparation of guidance material and so on—people have been working long hours and they have been working at home. I have been letting them have laptops and things basically to try to keep them working.

**Mr Yuile**—A lot of this is not necessarily accessing the system. People can be using—

**Senator LUNDY**—I know your information does not contain it, but can you tell the committee whether or not any other laptops have been stolen since from physical premises or from employees' homes since February 2003?

**Mr Yuile**—Not that we have information about. If you have information, Senator—

**Senator LUNDY**—I do not have information; I am just taking the opportunity to ask you to place that on the record.

**Mr Fisher**—I stand to be corrected but my understanding is that, other than the four, there was one other that went from somebody's home. But that was several years ago and a very different area.

**Senator LUNDY**—Is that on the list? The four that we have on the list are: in August 2000 a Dell note computer was reported stolen by a staff member—

**Mr Yuile**—Can I correct that while we are speaking? It was reported by a staff member as stolen.

**Ms KING**—You have got 'reported stolen by a staff member'.

**Mr Yuile**—We picked that up afterwards.

**Ms KING**—Okay, that is noted—the staff member did not steal it.

**Senator LUNDY**—The list says that the notebook in question was not recovered and the offender was not apprehended. The list continues: in April 2001, a staff member reported a notebook computer as stolen from an Adelaide hotel. The notebook in question was not recovered and the offender was not apprehended. Is there another notebook that was stolen from anyone's home?

**Mr Yuile**—Not that I am aware of.

**Senator LUNDY**—In terms of the department's compliance with the *Commonwealth Protective Security Manual*, can you say with confidence that all aspects of the PSM are complied with by both yourselves and your contractors?

**Mr Yuile**—We do everything within our power to ensure that we comply with the PSM. We issue guidelines, we run training programs, we remind staff of those obligations and we review our policy regularly. We take all those steps.

**Senator LUNDY**—Do you have a process that identifies actual or possible breaches of the *Commonwealth Protective Security Manual*?

**Mr Yuile**—In relation to?

**Senator LUNDY**—In relation to ongoing good practice.

**Mr Yuile**—For IT, for everything?

**Senator LUNDY**—I will ask the question generally and then I will ask it again specifically relating to IT. So the question is: generally, do you have a process that identifies actual or potential possible breaches of the *Protective Security Manual* as they occur, and do you document them?

**Mr Yuile**—We certainly keep the whole thing under active review. We run IT audits as part of our audit program. We have a very active IT committee, which has just reissued security policy in that area.

**Senator LUNDY**—Okay. Let me ask the same question in relation to IT security. Can you provide the committee with evidence of that level of accountability and assurance in relation to IT security—that is, that you do comply with the *Protective Security Manual*?

**Mr Banham**—We probably have not conducted an audit to ascertain our compliance purely with the PSM. We tend to look at functions and areas. The last audits that I am aware of have not indicated that we are failing the PSM.

**Senator LUNDY**—Can you confirm for the committee the status of the PSM? Is it a mandatory regulation?

**Mr Tongue**—The secretary is ultimately responsible for the storage of the information that we handle, but the PSM is, if you like—

**Senator LUNDY**—It is a guideline, isn't it?

**Mr Tongue**—Yes. But ultimately it is the secretary who is responsible.

**Senator LUNDY**—Does the department, as part of its security policy, invoke the PSM as a mandatory standard for the department, as is the ability of the CEO to do so?

**Mr Yuile**—Through our instructions, the CEI and other instructions, we certainly refer back to the PSM as the guiding document.

**Senator LUNDY**—But has the department adopted it as a mandatory standard? The committee has been led to believe previously that departments can choose to do that, although it is not provided by the Commonwealth as a mandatory standard. I understand that different agencies and departments can choose to adopt it as such and insist that it be applied to the letter, with all the risk assessment processes and so forth that it involves. I want to know whether your department has done that.

**Mr Fisher**—Maybe the confusion across the table, and the reason it is difficult to respond to your question, is terminology. The prescriptions for staff are set out in the chief executive instructions. Our chief executive instructions expect compliance with the PSM, so we refer to the PSM, we invoke it, we monitor against it. It guides, in an enforceable way, the behaviour of our people, but the authority for that is the chief executive instructions. That is the legal instrument by which the rules are enforced.

**Senator LUNDY**—Can you confirm your status with respect to the group 5 contract?

**Mr Yuile**—What do you mean by 'status'?

**Senator LUNDY**—Are you a member of the group 5 contract?

**Mr Yuile**—Yes.

**Senator LUNDY**—Have you extended that?

**Mr Yuile**—No.

**Senator LUNDY**—When is it due to terminate?

**Mr Yuile**—On 30 June 2004.

**Senator LUNDY**—In terms of the security arrangements within your contract with Telstra on IT, can you confirm that the sanctions within that contract, for failures in e-security related matters, consist only of the termination of the contract?

**Mr Banham**—I think I can confirm that. I will double-check when I get back. We looked at it recently, with this earlier event, and it triggers an early termination.

**Senator LUNDY**—Can you confirm whether or not the assets of DOTARS are now the assets of Telstra, as far as IT, hardware, software and systems go?

**Mr Banham**—Not necessarily software, but certainly the title of the hardware assets would be with TES.

**Senator LUNDY**—So all of your desktops, laptops and all those sorts of things are in fact assets of Telstra?

**Mr Banham**—That would be correct. There may be one or two exceptions—for example, where we have brought a specialist piece of equipment or inherited something that has come in.

**Mr Yuile**—That is the nature of the contract.

**Mr Fisher**—Could I clarify the answer to your question? Your question, Senator Lundy, was something like: 'Can you confirm that the assets of DOTARS are now the assets of Telstra?'

**Senator LUNDY**—The IT assets.

**Mr Fisher**—I am not quite sure what that means. We use Telstra assets.

**Senator LUNDY**—That is what I mean.

**Mr Fisher**—Yes, we use Telstra assets.

**Senator LUNDY**—I could also tell you, as I am sure you are aware, that when that contract was first put in place there was an asset transfer between yourselves and Advantra.

**Mr Fisher**—Five years later, I doubt that any of those assets would still be in use in the department. We now have access to Telstra desktops, laptops and service. This stuff belongs to Telstra.

**Mr Banham**—I would like to clarify one thing: most of those assets are actually leased again by Telstra, so they may not actually be titled to Telstra.

**Senator LUNDY**—Can you tell me the approximate value of the IT assets? Where I am heading to, of course, is where I headed to with an earlier witness—that is, in the event of a termination of contract as a result of a security breach, what cost would be incurred by the Commonwealth to replace those assets, given that they are not currently yours and you need them to do your job?

**Mr Fisher**—I hope I can answer your question, though I cannot, off the top of my head, give you a dollar figure. You would be aware that the department is currently market testing its IT. We will not have a good sense of what it will cost to provide IT in the department in the future until we have completed that process. When we have all the tenders in, assessed all the tenders and then matched them against our business requirements, we will have an idea of what the best alternative cost would be. But, until we complete that work, we would not know.

**Senator LUNDY**—The prospect of cancelling Telstra's contract as a result of security breaches is not a very credible one if you need to market test to actually determine what your possible costs are. Is that a fair comment?

**Mr Fisher**—The reality for us is that there were, as you know, options to extend the contract. We have opted to market test instead of automatically rolling over the contract. We looked at—as you would expect—the question of termination when the incident occurred.

**Senator LUNDY**—That is what I am going to now. You have had a major breach of security and you have obviously decided not to terminate the contract. So I put to you that you have no effective sanction against Telstra for major breaches of IT security.

**Mr Fisher**—We are market testing and we will find a new provider.

**Senator LUNDY**—Are you saying that a market test is a sanction?

**Mr Fisher**—We had an option to rollover and renew the contract, and we are not doing that.

**Senator LUNDY**—So market testing is your only sanction against Telstra for a major IT security breach?

**Mr Fisher**—I think Telstra would be a bit disappointed that we did not extend their contract.

**Senator LUNDY**—Is Telstra's disappointment an appropriate sanction in the circumstances that are described in the document—the loss of backup tapes; the fact that they were kept in a wheelie bin and allegedly thrown out with the rubbish? It is pathetic!

**Mr Fisher**—I will not react to that, but I will say that DOTARS was one part of a group. The contract was managed by the group as a whole. DOTARS has decided as a result of a lot of experiences, including the security incident, to test the market for alternative providers. Not everybody else in the group has elected to do that. DOTARS has actually taken steps to find alternative ways of getting its IT needs met.

**Senator LUNDY**—So in the mean time you still need to work with Telstra, because the reality is that you cannot excuse yourself from the contract at this point in time, regardless of the depth of the IT security breach?

**Mr Fisher**—The reality is that we made a business decision that we would be better off to test the market to find an alternative provider than to simply evoke the termination clause. It was a conscious business decision based on what was in the best interests of the department.

**Senator LUNDY**—I put it to you that you did not have any other option. You did not have an option to immediately terminate Telstra, because of the business impact that that would have on your organisation.

**Mr Fisher**—We made a business decision to market test.

**Senator LUNDY**—But it is a fair point, Mr Yuile. I note in correspondence to the committee you make this statement:

> In regard to this department, the Secretary, Mr Matthews, took up the issue directly with Telstra, seeking assurance from Telstra—Mr Thodey, Group Managing Director—that, as TES moved into the final year of the contract, services would not diminish and that a similar breakdown of procedures would not reoccur. Mr Thodey gave such an assurance.

I put it to you that that is the extent of the sanction able to be obtained under the outsourcing contract with Telstra in relation to IT security breaches.

**Mr Yuile**—Mr Fisher said what we have done. We have done what you would expect in terms of looking at that provision, looking at our business needs and conducting our business with the service provider to ensure that services are continued.

**Senator LUNDY**—One more question in this area: the audit report *The implementation of whole-of-government information technology and infrastructure consolidation and outsourcing initiative* into the group 5 contract said:

... Group 5 Agreements set out a framework of security obligations on the ESP—

Telstra—

and provide for the audit and inspection of compliance with those obligations, but do not include specific contractual obligations for the ESP to obtain external security certification of its systems. Neither Agreement identifies which party is responsible for the costs associated with obtaining external security certifications or assessments where agencies consider this appropriate.

Can you tell the committee whether, as a result of those findings of the Audit Office at that time, DOTARS pursued those external certifications relating to security for Telstra—it would have been Advantra at the time—and whether they were obtained?

**Mr Yuile**—My recollection is that they were, but I am not sure. I would have to take that on notice.

**Senator LUNDY**—Can anyone else at the table advise me?

**Mr Banham**—I can say that the department's main area of concern was Internet access. We moved those services to outside of the TES contract. They are now provided by a DSD certified Internet service provider.

**Senator LUNDY**—At the time—and I am sure you are familiar with this report—the Defence Signals Directorate advised the Audit Office:

The identification and then oversight of contractual obligations would therefore be even more resource-intensive than for conventional government networks.

This is in the context of outsourcing. It goes on to say:

Another point to be noted is the view that in the intelligence community, information security is a core management responsibility for which we must be held accountable, rather than a support function that can be offered up for external administration.

To what degree did DOTARS take that statement by DSD into account in the security clauses within your IT outsourcing contracts?

**Mr Fisher**—DOTARS did not negotiate the contract. DOTARS was doing the best they could within a contract. We have taken on board various experiences we have had with that contract and various audits and recommendations. In going to the market to provide an alternative

provider, DOTARS is clearly changing the arrangements under which its IT will be provided, including what is brought back in house and what is left with the external providers. Those recommendations, amongst others, have informed the way we have structured the new contract.

**Ms KING**—You have recently taken on a much stronger role within DOTARS for national security. Was any thought given at that time to revisiting your IT contract because of your new role in national security?

**Senator LUNDY**—And, importantly, were you able to under the group 5 contract structure?

**Mr Fisher**—The reality for us is that the contract has got less than nine months to run, and we have decided that we do not want to stay within that arrangement. The business decision for us is: do we put resources into scoping out a new contract that better meets our needs, given the current arrangements in the department, or do we attempt to renegotiate the 4½-year-old contract that we have already figured does not meet our needs? We have decided to put our emphasis on scoping a new contract arrangement that meets DOTARS current business needs.

**Mr Yuile**—To answer your question, Ms King, the enhanced role and the responsibilities that we have taken on are certainly informing that business case as well.

**Ms KING**—Mr Fisher, in relation to the pass that was lost by a cleaner who is part of a cleaning agency that has a contract with the building manager, you said that the lost pass 'was not our problem'. Those are your words. What measures have you put in place, given that it did become your problem, to ensure that things such as lost passes from the cleaners who have contracts with the building managers, or the security agents who have contracts with the building managers, are reported to you, that you know the personnel who are entering the building in terms of that cleaning contract, and/or whether or not the losing of a pass enables access into your areas of the building?

**Mr Fisher**—I was responding to your question 'What have you done to get the passes back?' or something like that. My answer was intended to indicate that DOTARS itself had no powers and no authority in respect of a building manager issuing passes to a joint tenancy area to its subcontractors—just so that people do not have an impression that I was implying that we do not care. We care, clearly, but we do not control the universe. We can control only those things within our boundaries, not outside our boundaries. I cannot control who walks down the street, and I cannot control who walks through the atrium in a common area that has joint tenants. That was the intention behind my response. What we have done is to ensure that we have more present guarding services within our boundaries. We have now got guards who patrol the perimeter and walk around inside the building 24 hours a day, because clearly there has been a public perception, based on some erroneous information, and we need to deal with that. If in the future somebody wants to walk from a common tenancy area and break our security barriers, then they will be confronted—whatever the time of night or day—with a guard.

**Ms KING**—That is a pretty costly laptop theft.

**Mr Fisher**—It is pretty costly uninformed public speculation.

**Ms GRIERSON**—As a group 5 participant in the contract that has had its backup tapes thrown away into the garbage, what has been lost and how have you responded to it? What specifically, for DOTARS, has been lost, and how have you responded to that?

**Mr Banham**—We have not responded as DOTARS. We have handled this as a member of group 5. I cannot talk on behalf of the other agencies—I am not aware of the contents of the tapes from their perspective—but we did not lose information as such.

**Ms GRIERSON**—It is still archived and still available.

**Mr Banham**—Yes, it is. A copy was lost. We lost basically the end-of-month backups from our email service. None of the other applications were involved.

**Ms GRIERSON**—If you are considering renegotiating a unilateral contract, just for DOTARS, you suggested in an answer earlier that there would be some things you would now recommend be handled in-house. What would they be?

**Mr Banham**—The security management is going to be back in-house—

**Ms GRIERSON**—And you will be recommending that it is not outsourced and it is handled in-house.

**Mr Banham**—We have already taken that out of scope in our market test.

**CHAIRMAN**—Thank you very much, gentlemen. I think you owe us some answers. If we have any further questions, you will not mind if, as usual, we put them in writing?

**Mr Yuile**—Mr Chairman, I am conscious in closing that, in my response, we also owe you responses from our portfolio agencies. I understand that three of those have come in today, and I will confirm them with you. There is one more to go, and I regret that we are running a bit behind time with those.

**CHAIRMAN**—Thank you.

[11.47 a.m.]

**BATMAN, Ms Gail, National Director, Border Intelligence and Passengers, Australian Customs Service**

**HARRISON, Mr Murray, Chief Information Officer, Australian Customs Service**

**WOODWARD, Mr Lionel, Chief Executive Officer, Australian Customs Service**

**CHAIRMAN**—Welcome. The first question I have to ask relates to your submission to us dated 12 September. The submission is in confidence. Are we not able to ask you questions on the public record today regarding that, or do I clear the room?

**Senator LUNDY**—I am sorry, Mr Chairman, can you say that again?

**CHAIRMAN**—The Customs submission is in confidence, and I am asking them whether we can ask questions regarding that submission today on the public record or whether I have to clear the room and take it all as in camera evidence, which means that we cannot use it when we report on this inquiry.

**Mr Woodward**—Mr Chairman, I think we would be happy to give evidence in public. If anything comes up with any particular sensitivity, could we seek your indulgence on that occasion?

**CHAIRMAN**—Thank you for that, Mr Woodward. We are all aware of the incident regarding the two servers at Mascot, Sydney. We are also aware that Ms Batman came back the next day to the aviation security inquiry and told us about that. I had heard it on ABC news in the morning on the way into the hearing, and I was not very happy about it. The following day we had a newspaper article in the *Herald Sun* regarding the theft of a laptop from DOTARS. I have to say to you that, immediately after the DOTARS incident appeared in the *Herald Sun*, I had a telephone call from the Deputy Secretary of the Department of Transport and Regional Services, apologising and telling me what had happened, and immediately following up with a letter. I still have had no apology from Customs, and I would like to know why.

**Mr Woodward**—I do apologise now. The only explanation I can give you, Mr Chairman, is that we did then and have now looked at the terms of reference of the aviation security inquiry. We did not see a relationship between the terms of reference for that inquiry and the theft of computing equipment from an office building adjacent to the Sydney airport. Obviously you did not share our judgment, and to the extent that the committee believes we should have passed on that information, I do apologise.

**CHAIRMAN**—Ms Batman did say to us on the public record that day:

> We did expect that immediately after the incident the story would be in the press. When it did not appear, we all assumed that it would not. If it had not been for this leak—I do not think this is an appropriate matter to be canvassed in public in the middle of an investigation.

You know that we are conducting an inquiry into IT security. You are well aware of that. Do you really believe it is appropriate to tell us that the committee is not entitled to know about an incident such as this?

**Mr Woodward**—We drew a distinction which was obviously wrong. There was a public accounts committee hearing into aviation security with a particular set of terms of reference. We thought 'Is this something that is appropriate to be brought before that committee with those terms of reference?' We did not believe that there was a relationship, as I said. To the extent that we are wrong and if there is an obligation not to divide up the committee in the way in which we have, between an IT security related hearing and an aviation security hearing, then, as I said, I apologise.

**CHAIRMAN**—Okay, we will move on. You said in your response to the incident itself:

The backup domain controller contained an encrypted list ... An external attack, or intrusion, into Customs network using these lists is not possible due to firewall protocols.

Are you confident that the firewall is absolutely impregnable?

**Mr Woodward**—I would make a couple of observations that I think are important, which pick up this question; I have other experts with me. This whole thing really has been evolving. We found a theft, which we took seriously and immediately involved the New South Wales police, as it was regarded a theft of items of equipment. We then very quickly established that the potential was to go beyond a mere theft of the equipment and we involved the Australian Federal Police, who took over responsibility for the investigation. That investigation has been finalised to the extent that people have been charged. An initial court appearance has taken place, and further court appearances will take place in mid-November. It is possible that further investigations by the Federal Police in relation to the theft are continuing.

We also sought to involve the Defence Signals Directorate in their capacity as the information technology security adviser to the Commonwealth—in other words, discharging their statutory role. They have been involved, but they have not presented a final report. Obviously we have been working very closely with them, and they in turn with the Federal Police. Another inquiry was set up by the government, and we have been cooperating with that inquiry, and now we have your own interest. The difficulty that I have is that some of the inquiries have not been completed. Information that was established early on in the process, because there were demands through the media and through the normal ministerial process for information, evolves as more information comes in from the police, from an external inquiry or from the Defence Signals Directorate inquiry. The information that we have now, which is still not finalised, might change even more when these other inquiries come to fruition.

**CHAIRMAN**—You are aware that this committee takes this issue very seriously—so seriously, in fact, that we reopened this inquiry because of it.

**Mr Woodward**—Yes, indeed.

**CHAIRMAN**—We made a snap, on-the-spot, decision that day to do so—at least the sectional committee did—because, in a sense, we did not question people about the physical

security arrangements surrounding their computing equipment and national security issues. You have a contractor that operates the facility where the two servers were stolen from, yet you are responsible for the physical security of that building. Is that correct?

**Mr Woodward**—Physical security in Customs is a Customs responsibility. The contractor—in this case, EDS—and any other contractors that are working in a Customs environment are required to comply with our security instructions and our guidelines, which are moulded around the *Protective Security Manual*. To the extent that there has been a failure—and I am not denying there has been a failure—we will face the prime responsibility of being accountable for that.

**CHAIRMAN**—How did they get in?

**Ms Batman**—It would appear that they posed as employees of a subcontractor of EDS. They understood what they needed to do. They went to level 3, at the Link Road building, at about four o'clock on 27 August and asked specifically for the key to the communications room nearby. They asked for it by name. They were asked to sign in a book for the key. It is called a key, but it is actually a swipe access card. There is also a key to another communications room in the basement—so it is a bit variable—but access to that room is through a swipe access card. They accessed the room that way.

**CHAIRMAN**—I know aviation security is a different inquiry, but how difficult would it be for someone to pose as one of your subcontractors, go airside at Mascot and access either computer information and sensitive Customs information or aircraft?

**Ms Batman**—The access arrangements at the airport are under the control of the Sydney Airports Corporation. Customs works on that site. The access control arrangements to the secure areas are through an aviation security identity card, which is controlled and issued by the Sydney Airports Corporation.

**CHAIRMAN**—Unless it is a day pass?

**Ms Batman**—Yes, there are visitors' passes.

**Senator LUNDY**—So the card that was obtained was issued by the Sydney Airport Corporation?

**Ms Batman**—No, not in Link Road—not at this site. I was responding to the Chairman's questions about general access to the airport by contractors.

**Senator LUNDY**—So the contractors would have had to have had—

**Ms Batman**—A visitor's pass.

**Senator LUNDY**—Was that established in the course of the investigation?

**Ms Batman**—No. The building that they accessed was not part of that airport; it was adjacent to the airport. The access control was granted by a Customs officer who was working at the public access counter on that floor.

**CHAIRMAN**—If I remember correctly, you told us that that building is on the perimeter fence—

**Ms Batman**—It is.

**CHAIRMAN**—and there is access from the airport and there is access from outside.

**Ms Batman**—I was incorrect: there is a gate nearby that you can access, but it is a secure gate.

**CHAIRMAN**—But your computers were supposed to be under a secure environment.

**Ms Batman**—The building is next to the airport. There is no direct access from the building into the airport fence.

**Mr Woodward**—I would stress, Chairman, that there is no doubt that there has been a serious breach, and we would not attempt to put to you that there has not been a serious breach. We have a comprehensive set of security practices that are required to be followed—and are generally followed—which, I think, meet the standards that any external agency would set. In essence, what happened was a breakdown in the process in a particular location. That should not have happened. It was a process that had evolved over a period of years. So it is not something where one could single out a particular individual and say, 'You have messed it up on this occasion.' It was a process that had evolved which should not have evolved—it was inconsistent with our security manual—and we have already taken steps to deal with it.

We have taken physical steps to deal with access to the building, security steps in relation to the computer room and steps in relation to accompanying people when they go on site. Many steps have already been taken. We have also said that if it can happen at Link Road, it could happen elsewhere. So we are having a comprehensive look at security throughout Customs, with one of the major requirements being security plans which will be site specific—so that each site will need to have a security plan and an obligation that the security plan is complied with. We are not attempting to say that this is not serious—it is and it is extremely embarrassing.

**CHAIRMAN**—I sent a letter to you—as well as to every other agency in the Commonwealth—asking about thefts, and we have not as yet had a response from you.

**Mr Woodward**—We have contributed to an Attorney-General—

**Senator LUNDY**—There is a response; it is part of the response from the A-G's. I have read it and I have some questions about their response.

**CHAIRMAN**—Sorry, we received the response this morning—and I obviously have not had any time to look at it. Has there been another incident involving mainframes or major computing equipment?

**Mr Woodward**—I stress that these are servers.

**CHAIRMAN**—Your submission to us says that they are powerful mainframes in themselves and they have monetary spare parts value for prospective thieves.

**Mr Woodward**—I accept what you are saying, but I would describe them as servers.

**CHAIRMAN**—A server is a computer. What else is it?

**Ms Batman**—It is not a mainframe.

**Mr Harrison**—It is not a mainframe. A mainframe is quite a large—

**CHAIRMAN**—I understand that a mainframe has a very large storage capacity. But these servers are computers.

**Mr Harrison**—They are all computers but these servers are very similar in size to a desktop computer.

**CHAIRMAN**—Have you had any other major incidents—because it is major computing equipment; it is not a laptop?

**Mr Harrison**—No.

**Mr Woodward**—There is a list that has been provided to you. The police investigation has indicated that, at the same time the servers were stolen, two desktop computers and a battery charger were also taken. There is no suggestion of anything on them that could prejudice security, as they were 'hot swap' computers—where you take out bits and pieces and you can use them for other purposes. We have given, in the Attorney-General's response, a list of computer thefts. There have been quite a few—and I understand that Senator Lundy has got some specific questions she wants to raise—but this is, in our view, the most significant theft of this kind which has occurred since I have been in Customs and, as I have said, we have treated it extremely seriously.

**CHAIRMAN**—The concern, at least from my viewpoint, is that while some mainframes are so large that getting them out of the building is going to be very difficult, there are mainframes which are small enough that you could put them on trolleys and get them out of buildings. If they can take the servers, then they could take very powerful computers that have hard drives that are full of all kinds of data that could be sensitive.

**Mr Woodward**—Yes, it is true, and it brings out the linkages between physical security and information technology security. My own view happens to be—and I am not sure whether it is shared by anyone else—that it is going to be extremely difficult for any agency or private sector organisation to come up with a foolproof mechanism that prevents theft from either buildings or homes. What it does do is put a lot more pressure on those who design systems to enable appropriate protection and a series of layers of security to be built into those computers, and into the software that lies behind them, in the event that they are stolen. I just do not believe that there will ever be a solution to theft. We do the best we can.

**CHAIRMAN**—In reviewing your security procedures following this major breach, have you made changes to the way you operate now?

**Mr Woodward**—We have made a large number of changes already. I mentioned some of them briefly. In terms of Link Road, there have been massive changes already, which would be very obvious to you.

**CHAIRMAN**—That might be described as 'after closing the barn door'.

**Mr Woodward**—I accept that.

**Ms GRIERSON**—The submission we received today, which we have not had much time to look at, says:

In January 2003 two EDS desktop PCs were reported as missing from Link Road, Mascot.

This suggests to us that perhaps a better response in January 2003 may have overcome the loss of these as well.

**Mr Woodward**—I accept that entirely. We have learned from this. We did not learn quickly enough from other events that occurred, but we have learned a great deal from what has happened on this occasion.

**Ms GRIERSON**—Adding to the Link Road site, those accused of the thefts allege they took two other items of equipment that you have not yet verified.

**Mr Woodward**—This is in relation to the recent one. That is the one that I mentioned a few minutes ago. It has now been established—and this is why I say it is an evolving picture, as we get reports in from the police, DSD, the external inquiry and our own investigations—

**Ms GRIERSON**—But you must have an asset register that would show what equipment is there.

**Mr Woodward**—The asset registers, in relation to computing equipment, are the responsibility of EDS. But it is clear that the asset register process was not good enough to enable us to establish with certainty, at the very beginning, that those additional items had been stolen. Again I am embarrassed that we—

**Senator LUNDY**—So this was on the same day that the two servers went missing.

**Mr Woodward**—The information we now have is that two servers, two desktop computers and a battery charger were stolen. The two desktop computers were hot swap computers and there was a brand new battery charger.

**CHAIRMAN**—Does all this national attention reinforce your belief in democracy—in an open and free press? In a closed society, you could have kept this quiet and nobody would ever have known.

**Mr Woodward**—Whether it would have been publicly known is one thing; what was clear was that we regarded it sufficiently seriously that we had in the New South Wales Police, then the Australian Federal Police and then the Defence Signals Directorate. We informed Australian Security Intelligence Organisation and our minister before anything hit the media. We had done a lot, and we had already started processes for corrective action. I do not think anyone likes adverse publicity.

**Senator LUNDY**—Going to the issue of the asset register, we have established with other witnesses that with the outsourcing arrangements we are in fact talking about assets that have been transferred at some point, either in their present physical form or at least as far as the system goes, to the outsourcing vendor. Can you confirm that that is the case with the IT assets in Customs?

**Mr Woodward**—I think that is the case. All of our assets were transferred to EDS. I did listen to the question you asked other witnesses. If I can draw one exception, it is not a transfer. We in our organisation have a number of the items of extremely sensitive, intelligence related connections to other organisations, which the chairman will have seen. Some of those were built and developed with the aid of defence or intelligence agencies. So there are some exceptions but, largely, they are with EDS.

**Senator LUNDY**—At what point in the investigation about the two servers did you become aware that two desktop computers had also gone missing?

**Mr Woodward**—There was an initial indication that there might have been some computer equipment that had gone missing. That was my own knowledge. We did some checks with the owners of the equipment.

**Senator LUNDY**—EDS?

**Mr Woodward**—Yes.

**Senator LUNDY**—When did you ask EDS whether anything else had gone missing?

**Mr Woodward**—There were a number of questions asked at various stages during the investigation.

**Senator LUNDY**—Was the question asked of EDS at that time whether anything else had gone missing?

**Mr Woodward**—It was raised with EDS reasonably soon afterwards.

**Senator LUNDY**—That day?

**Ms Batman**—The next day.

**Senator LUNDY**—What did they say the next day?

**Mr Woodward**—My recollection was that we had been told that other equipment might have gone. We asked EDS what had gone. Information we had, at least for a period, was that it was the two servers.

**Senator LUNDY**—Just to clarify that: you were initially told by EDS that it was only the two servers that had gone missing?

**Ms Batman**—The information EDS provided at the initial incident response team meeting that was set up was that the two servers had gone missing.

**Senator LUNDY**—And nothing else?

**Ms Batman**—At that stage.

**Senator LUNDY**—At what point did EDS inform Customs, if ever, that in fact two desktop computers had also been stolen at the same time?

**Mr Woodward**—I will need to be careful on one part of this. There was information obtained as part of the police investigation, which I do not want to go into but which led us to again raise the question of what might have been stolen. We went back to EDS—that is my recollection—and had confirmation that two desktops and a battery charger had been stolen.

**Senator LUNDY**—I put it to you that EDS never informed Customs of the missing desktop computers—that, in fact, it was only via the AFP investigation and Customs further querying EDS that EDS was able to confirm that they were missing. EDS was never in a position to, or chose not to, volunteer that information.

**Ms Batman**—At the time of the incident, I think there was some thought by the New South Wales EDS field service officer that there may have been such equipment in the room. That was discussed with Customs officers in New South Wales at that time. I think it was perhaps left at that level. I understand that, as part of the initial report to the New South Wales Police, the possibility of other items was canvassed at that stage. However, once the incident response team was established in Canberra, a different group of EDS people said that it was the two servers. From then on I think attention focused on those two servers.

**Senator LUNDY**—So what you are saying is that, in New South Wales, at the level at which it was first noticed, there was speculation about the possibility but that information was never transferred into the incident response team?

**Ms Batman**—Apparently not.

**Senator LUNDY**—Can you give me the date that the AFP advised Customs about the desktop computers?

**Mr Woodward**—We would need to check that.

**Senator LUNDY**—Can you give me the date at which Customs was finally forced to acknowledge that two desktop computers were stolen in the same incident?

**Mr Woodward**—Forced to acknowledge?

**Senator LUNDY**—Internally, through this incident response team and so forth. When did you say, 'Okay, now we know that two desktop computers were also stolen'?

**Mr Woodward**—We will tell you at what point we were convinced that the theft extended beyond that. There is one other point that I could make in terms of indications to EDS. As I have said, Chairman, I have been very concerned about this. I have had a number of discussions with the head of EDS in Australia and others about the issue. In one of the early discussions I did mention that there had been rumours of other computers being stolen. It was an earlier discussion and I was not aware of any of that. I would not want you to think that there were not early rumours, because that is all that I had heard. The realisation that they had been stolen was in fact very recent, and we now acknowledge that.

**Senator LUNDY**—Was that realisation—

**Mr Woodward**—We will give you that information.

**Senator LUNDY**—Was it yesterday, three days ago, a week ago, a month ago?

**Ms Batman**—It was about a week ago.

**Mr Woodward**—We did not know last week.

**Senator LUNDY**—So you only realised in the last week that two desktop computers were stolen?

**Mr Woodward**—Not realised—established.

**Senator LUNDY**—What was EDS's role in establishing that? Can you tell me whether they had an asset register and whether your difficulty was getting information from EDS or whether EDS themselves had difficulty in tracking their assets?

**Mr Harrison**—What we are talking about here is who knew what when. The local on site EDS person reported the two PCs the next day, as a result of their information about what assets were held in that room. That information was not passed through to the EDS executives in Canberra who were party to the incident response team that Ms Batman talked about.

**Senator LUNDY**—So you have identified the breakdown in EDS's security processes?

**Mr Harrison**—We have received an apology from them in terms of their communication around that.

**Senator LUNDY**—When did you get that apology from them?

**Mr Harrison**—We got an apology from the account executive of EDS.

**Senator LUNDY**—When?

**Mr Harrison**—On Wednesday of this week.

**Senator LUNDY**—So you established a week ago that two PCs were stolen in the same incident—at the same time the two servers went missing—and you received an apology for that on Wednesday?

**Mr Harrison**—No, we received an apology in relation to the information not being relayed to the incident response team at the time.

**Ms GRIERSON**—So who was that information initially relayed to?

**Mr Harrison**—It was relayed to the local Customs people on site in New South Wales and the New South Wales Police.

**Ms GRIERSON**—And they did not pass it on to anybody else?

**Ms Batman**—Yes, but the EDS people in Canberra had confirmed that it was two servers only at that point.

**Ms GRIERSON**—You were dealing directly with EDS to get that information?

**Ms Batman**—At both levels, yes.

**Ms GRIERSON**—Even though your own personnel had different information.

**Ms Batman**—Yes.

**Mr Woodward**—Can I again stress that investigations were going on at the same time and were crossing over each other. We had a state police investigation and a Federal Police investigation, our own internal affairs people were involved, DSD and ASIO were informed and there was an external review, with information passing between all of them because of the seriousness of it. We have done the best we can to explain what actually happened.

**Senator LUNDY**—Obviously it has been a complete debacle, and I am sure you are very embarrassed about the fact that you have only just discovered that two more computers went missing. I want to know what is the role that EDS played in that and why on earth Customs were not able to establish at the time that the theft had occurred. I can make some assumptions: Customs was not in a position to make any assessment about any of the assets under the control of EDS. I think that raises a whole series of questions about asset management within the department, from very basic security right through to national security. I am also very interested to know the process by which EDS found out themselves and whether they had bothered to inform you about the breakdown within the processes and procedures of EDS, which meant that you had to wait until October to get that information established from EDS. Did EDS just not bother to tell you sooner? What happened?

**Mr Woodward**—The best that we can put to you is, basically, that we have already done it. There were certainly rumours, or the information that had come in, as Mr Harrison has mentioned—

**Senator LUNDY**—I do not mean to interrupt, but we are talking about August, when they went missing. It is now October.

**Mr Woodward**—But you are also raising issues of internal communication within EDS.

**Ms GRIERSON**—Mr Chairman, I would like to ask a supplementary question to that. Internal communications should be part of a risk management and risk assessment response. When you have an incident, one of the standard responses in management procedure is that you control the communication flow. It seems that in this case, in terms of your risk management processes, the communication flow was not controlled and certainly was not directed correctly, or that information would have been in your hands a lot sooner. So doesn't that show that perhaps you have to revisit not just your security and outsourcing contracts but also your whole risk management approach in your department?

**Mr Woodward**—I can agree with some parts of what you are saying, but I think you need to understand that parts of the process are not Customs. We did not conduct the Federal Police inquiry into this matter. We are in effect the agency that had the building from which assets were stolen. We brought it to the attention of the Federal Police, and initially to the attention of the New South Wales police. We are only given during the course of any investigation the information that the AFP believe is appropriate. That information could not prejudice the course of the investigation, which I can well understand. DSD had been pursuing its work professionally, and we had no control over that, and we certainly had no control, although we cooperated fully, over the work of the external committee.

**Senator LUNDY**—Can you answer my question about the role that EDS played and why, in your opinion, you did not receive that definitive information from EDS until October?

**Mr Woodward**—All I can do is produce conjecture because I am not sure. We have had a breakdown in security. This may have been a simple breakdown in the assets management process on the part of EDS. I do not know whether it is a one-off or whether it is systemic. You are asking for information, and I just cannot give you any more than I have already told you.

**Senator LUNDY**—Let me be very clear about my point: do you think EDS attempted to cover up the theft of these two PCs?

**Mr Woodward**—My personal view is no.

**Senator LUNDY**—Have other views been expressed?

**Mr Woodward**—Not to me. You have two people here who can say what they think. I have no reason to believe that there has been a cover-up.

**Ms Batman**—My view is that I would agree.

**Senator LUNDY**—So you think it is just incompetence, as opposed to a cover-up?

**Mr Harrison**—No.

**Senator LUNDY**—It is one or the other, isn't it?

**Mr Harrison**—There was a breakdown in communication, but on the issue of a cover-up there is also no doubt that the focus of everybody was on the servers and not on the PCs, which we recognise.

**CHAIRMAN**—Does EDS have an asset register?

**Mr Harrison**—Yes, they do.

**CHAIRMAN**—Do you have access to that?

**Mr Harrison**—We have access to that in that we are able to audit it.

**CHAIRMAN**—If I had had a break-in like that and had had all this national publicity, the first thing I would have done would have been to go to the asset register and figure out if they had taken anything else.

**Mr Harrison**—Indeed.

**Senator LUNDY**—It is inconceivable that this has occurred without at least a concession from the department that it was the complete incompetence of EDS or, alternatively, that EDS withheld that information from the department and from the investigations until last week. I think this committee really needs to know which one it was.

**Mr Woodward**—You are asking whether it was one or the other, and I think it was possibly something else. I have no reason to believe there was a deliberate decision on the part of EDS not to pass information on, nor am I saying—because these things do happen—that it was incompetence. It may have happened—and I have acknowledged this—that there was a breakdown in practice or procedure. That may have been the cause of it. I do not believe that you must say one or the other, when I honestly think the answer may well be a third one.

**Senator LUNDY**—Is there any investigation occurring into the possibility of there being a cover-up on behalf of Customs' IT external service provider?

**Mr Woodward**—There certainly is not at the moment. With the number of inquiries that we have going in the area and with some of those inquiries not yet completed—in fact, the majority of the inquiries not yet completed—we are not embarking on an exercise as to whether or not there has been a cover-up in circumstances where I have no reason to believe that there has been a deliberate cover-up.

**Senator LUNDY**—Going to the question asked by my colleague Ms Grierson, can you tell me what the provisions of the contract with EDS provide for with regard to audit of assets?

**Mr Woodward**—In relation to security?

**Senator LUNDY**—Indeed. I will come to that.

**Mr Harrison**—We are required under the contract to review EDS procedures in a number of areas. We have the freedom to audit their activities, and we have done so over the years. I think we have carried out something like 17 in the last four or five years.

**Senator LUNDY**—Can you tell me whether Customs is in a position to know whether or not assets have gone missing, in the light of what has occurred with these two PCs? I put it to you that the procedures surrounding the theft of these two PCs and the fact that it was not reported in a timely way leave open the possibility of other assets having gone missing without EDS knowing about it let alone any investigating authority or Customs. What can you tell the committee to guarantee that has not happened?

**Mr Harrison**—I am a little uncomfortable in the sense that I am sure EDS would argue that they reported this the next day. What occurred was a failure to communicate that information to the senior people in Canberra—

**Senator LUNDY**—My question still holds. What if EDS, at the grassroots level throughout the organisation, reported it and it was not reported through? The query is still valid. How can you guarantee that this has not happened in other cases?

**Mr Harrison**—The event has focused the mind about asset management in Customs. Since this particular event, there has been an extensive audit of all of the equipment across the Customs network by both EDS and Customs. We now have perhaps the most up-to-date information in relation to our asset holdings. I am sure you would appreciate that that is a dynamic environment.

**Senator LUNDY**—When did you do that audit?

**Mr Harrison**—Within the last month.

**Senator LUNDY**—Can you tell me whether it was that audit that exposed the fact that these two PCs were missing?

**Mr Harrison**—No, this was an audit in response to the event to make sure that we knew what we had.

**Ms GRIERSON**—Can you tell us when your last audit was of that contract or of the assets on the contract?

**Mr Harrison**—I would need to take that on notice.

**Senator LUNDY**—Just to clarify this, you established last week that the two PCs were missing. You got an apology about the issue from EDS on Wednesday, but you say there was an extensive audit done over the last month. Did that audit expose the fact that the two PCs were missing?

**Mr Harrison**—No, the audit was not a reconciliation against the previous asset register. This audit was: what do we have where. I did count them, in other words.

**Senator LUNDY**—So you established a new benchmark of assets.

**Mr Harrison**—Yes.

**Senator LUNDY**—That implies that there was not a previous asset register. Is that the case?

**Mr Harrison**—We did not do a reconciliation between the previous asset register with the current one—

**Senator LUNDY**—Why not? That would have shown that these two PCs were missing, and such an exercise would show if anything else was missing that has been missed.

**Mr Woodward**—I think the assumption of that question is that assets remain where they are forever. These assets are being moved around all the time—

**Senator LUNDY**—With all due respect, there is pretty sophisticated asset management software now that can account for those sorts of things. That is not an excuse.

**Mr Harrison**—Let me qualify my answer. With the audit that was conducted to determine what we had where, there was follow-up in relation to the results as to whether they were significantly different from what we thought was there.

**Senator LUNDY**—So you did do some comparison with the previous assets.

**Mr Harrison**—As I understand it.

**Senator LUNDY**—Did that, or did that not, show up the fact that the two PCs were missing?

**Mr Harrison**—That exercise did not, in itself, alert us to the issue of these two PCs.

**Senator LUNDY**—Does that concern you?

**Mr Harrison**—One needs to be concerned, but I am also conscious of the environment. It is not an unusual situation for PCs—particularly desktop PCs, particularly laptop PCs—to not be in the place you think they are, in an environment like this.

**Senator LUNDY**—But is it unusual for them not to show up on the asset register at all?

**Mr Harrison**—As I said, I do not believe that we did the reconciliation to a level that would show that in this exercise. We were not trying to do that; we were trying to find out what we have now.

**Mr Woodward**—The other obvious point I should make—and it is obviously clear in your mind—is that some of the assets we are talking about are assets used by EDS for them to do their work, as distinct from assets that are otherwise Customs assets.

**Senator LUNDY**—I appreciate that, but what I think is well understood by committee members now is the nature of the outsourcing contracts that involve the transfer of those assets. There is obviously no distinction between a computer that a Customs officer is working on and a computer that an EDS officer—in supporting that Customs officer—is working on. There is no distinction for the purposes of the EDS contract. Either way, EDS, I presume, with Customs holding them to account, are responsible for that asset register. So I put to you that it should not matter who is using it; that data should still be kept accountable, auditable and you should be able to report to a parliamentary committee about the status of it. What I am hearing now is that that is not possible and, where it has been attempted, it has not shown up obvious theft.

**Ms GRIERSON**—Senator Lundy, could I add to that. Regarding your assets, I note from the information you provided us today that two encryption modems were lent to DIMIA—I do not know if DIMIA use EDS or not. Do they?

**Mr Harrison**—No. Not as their prime contractor, certainly—

**Ms GRIERSON**—I am wondering whether your contract allows you to lend encryption modems that then end up with DIMIA but then end up in a garbage dump. Were those identified very quickly? How do you show to EDS that two encryption modems—do they belong to you or to EDS?—go missing or are lent out to another department and then go missing? What is the contractual process for that?

**Mr Harrison**—I am not familiar with that.

**Senator LUNDY**—Just for the sake clarity: Customs have provided—as part of A-G's submission to this inquiry, which was published today—a list of a series of incidents, numbered one to 14, of various thefts of laptops, line encrypters and of other security incidents. The list includes the two IT servers but does not include the two desktop computers that we have been discussing today. I would like the opportunity to go through each of these incidents.

**Mr Woodward**—I think it does include those.

**Senator LUNDY**—It does include the two?

**Ms Batman**—Yes.

**Senator LUNDY**—Where is that, please?

**Ms Batman**—In No. 9.

**Senator LUNDY**—It says 'two other items of computer equipment'. You did not specify desktop computers; it just says 'two other items of computer equipment'. There was one other item as well, wasn't there?

**Mr Woodward**—Yes, a battery charger.

**Ms GRIERSON**—Could you tell me how that exchange of equipment between two departments using separate contractors can happen and whether you think that is a wise process in terms of managing assets?

**Mr Harrison**—I am advised in relation to this incident that we lent those encrypters to DIMIA to test the connection between DIMIA and us. They were not used in a production environment; they were used in a test environment to make sure that the link worked. In that exercise they were lost.

**Senator LUNDY**—No. 6 of the list says:

In January 2003 two EDS desktop PCs were reported as missing from Link Road, Mascot. The incident was not reported to the police by Customs as the computers are EDS property, did not contain Customs information and were never used by a Custom's employee. The items have not been recovered.

Given that we have established that just about every piece of hardware used by Customs is in fact owned by EDS—and I concede that there are some items that are not—and, whether or not a Customs officer uses it, there is a chance that Customs related information is potentially associated with that, why have Customs drawn out this distinction of not reporting that incident to the police by virtue of the fact that it is not an asset of Customs, when we now know that most of it isn't?

**Mr Woodward**—The only explanation I can give is that there are dual responsibilities. If an item of equipment clearly owned and run by EDS is missing, there is a responsibility that EDS has, and its security people have—

**Senator LUNDY**—But how is that different to the servers? They were EDS assets.

**Ms Batman**—These computers contained no Customs information at all.

**Senator LUNDY**—How do you know that? You did not report it to the police. Did you investigate it?

**Ms Batman**—That was the advice from EDS.

**Senator LUNDY**—EDS told you that?

**Ms Batman**—They were their computers that they used for their work.

**Senator LUNDY**—So you took EDS's word for that, without doing an independent investigation?

**Mr Woodward**—It is one of the natural consequences of an outsourcing arrangement that, unless you duplicate the organisation—in this case EDS, but be it IBM, CNC or whatever—you come up with a set of arrangements that are designed to work as best they can but without one looking over the shoulder 100 per cent of the time. What we aimed to do was to have a set of

processes and audits which enable us to satisfy ourselves that the arrangement is working properly.

**Senator LUNDY**—That sounds to me like a confession that it is not working properly and that your efforts to outsource the risks associated with security have not been as effective as you would have liked.

**Mr Woodward**—That is not what I intended to say. In an organisation the size of Customs, where virtually everything we do runs on computers, things do not always work perfectly. The point that I think is behind the comment you are making deals with outsourcing. Before we went to an outsourcer we had many contractors working in Customs and we had many breakdowns caused by our own people or by individual contractors, including some that hit the press. So, in my view, there is no perfect arrangement.

**Senator LUNDY**—Can you tell me whether EDS reported this theft to the police and whether there was any—

**Mr Woodward**—With this particular one, my understanding is no.

**Ms Batman**—That is also my understanding.

**Senator LUNDY**—So two EDS desktop PCs went missing from Link Road. Is that the same physical location that the two servers went from.

**Mr Woodward**—The same physical location, yes.

**Senator LUNDY**—So, previously, two PCs went missing and no-one bothered reporting it to the police?

**Mr Woodward**—That was a point that was made earlier. I accept that there were warning signs that we should have acted on and we did not.

**Senator LUNDY**—I appreciate that in relation to this, but I am really concerned that there have been thefts that were not reported full stop, let alone about the signals that that subsequently gave you about the vulnerabilities in Customs.

**Mr Woodward**—All we can do is give you the facts as we know them. They did go. As we understand it, they did not contain Customs information and, as we understand it, were not reported.

**Senator LUNDY**—But you only have the word of EDS on that.

**Mr Woodward**—We have the word of EDS on that. But obviously if you wish to pursue it, we can follow it up.

**Mr Harrison**—It is the word of EDS, but they were brand-new computers that had not been taken out of the box.

**Senator LUNDY**—Do you have a report on this incident?

**Mr Harrison**—That is the advice from EDS.

**Senator LUNDY**—One of the issues for this committee is that EDS of course says that the arrangement is that the agencies and departments themselves will report back on the details of incidents. So this morning we were unable to query EDS specifically on this. What we have been able to establish is that there may well be incidences that are not reported to the police, as in this example. How can you be sure that other things are not occurring within EDS that Customs is not even informed about? How do you know that?

**Mr Woodward**—If you are talking about absolute knowledge, which I am not sure exists anywhere, I do not think we can be absolutely sure. But what we have is a set of relationships, under the broad umbrella of the contracts, which have developed over the years. We have a set of working relationships, which I believe are now sound, between our management people and EDS management in which we are as confident as we can be that if major things were to go adrift we would find out about them. But, as with anything, things go wrong. You have seen examples today.

**Senator LUNDY**—I would like to turn to item seven in the additional submission from Attorney-General's, which states:

In April 2003 a briefcase containing a keyed randata encryption modem was lost. The briefcase was placed on a Qantas aircraft as cargo at Broome but could not be found on arrival at Darwin. The incident was investigated by IT Security, however neither the briefcase or modem were recovered. The encryption codes were changed to remove any risk of the modems being used to access Customs networks.

Can you tell me for comparison purposes whether EDS were involved in that at all? What were the reporting procedures that Customs followed at the time of that incident?

**Ms Batman**—No, EDS were not involved in that instance. It was an officer travelling who had two pieces of equipment that they wanted to keep with them at all times, including this set. The airline would not let them take both items onto the plane. They had to choose to put one in cargo. It did not turn up. Inquiries were made, it was reported and steps were taken to report it to DSD so that it could be reset so that the encryptor and encryption codes could not be used.

**Senator LUNDY**—So DSD were involved in that.

**Ms Batman**—We reported that at the time, as we needed to. It was an unfortunate incident. The officer was in a difficult circumstance at the time and made a judgment. Unfortunately, it went wrong.

**Senator LUNDY**—The report says that the briefcase and the modem were never recovered.

**Ms Batman**—That is true, but they have been reset.

**Senator LUNDY**—Was ASIO involved in that investigation?

**Ms Batman**—No, it appeared to be an airline lost luggage item rather than anything more sinister. It was a spur of the moment decision.

**Senator LUNDY**—Did it fall out of the plane or something?

**Ms Batman**—I am sure airlines lose luggage. It was one of those incidents rather than anything else. It was, unfortunately, a lost luggage incident.

**Senator LUNDY**—That means there have been some seven laptops that have gone missing over time.

**Ms GRIERSON**—I have a few more questions I would like to ask. Ms Batman, when you appeared before the committee in September, you were asked what information would be accessible through those file servers; and you did not know at the time. Your new submission says that you are confident that they would not provide access to national security information, however all passwords were changed in response to those incidents. Can you now tell me more precisely what information would be accessible if those file servers were then plugged into a computer, et cetera?

**Mr Woodward**—The short answer is that we will not know with any certainty—it is one of the things that, as I have mentioned, is evolving—until, firstly, a final report is lodged with the minister, not with us, by the external reviewers; and, secondly, until after DSD has been able to complete its work. Its work has had to tie in with the police investigation and the availability that the police require for basic hardware and related gear.

**Ms GRIERSON**—Do you know at this stage if that information has been breached or accessed?

**Mr Woodward**—We have no reason to believe, at this stage, that there has been any breach of national security or operational security as a result of the theft of the servers. All the indications at this stage—and we stress that we will not know for certain until all this other work is completed—are that it was a theft.

**Ms GRIERSON**—But you are concerned about the pay system being accessed.

**Mr Woodward**—We were sufficiently concerned about this, including the possible national security and other implications of it, that we brought in DSD, we notified ASIO, we brought in the Federal Police. We will not know for sure until all that work has been completed.

**Ms GRIERSON**—However, you did not take it seriously enough to tell DIMIA—who also share that information—that that had been breached. There was a two-week period and they found out through us, basically.

**Ms Batman**—It is a level of communication as to who in DIMIA knows, but there are 150 DIMIA staff who work at airports and who changed their passwords as a result of this incident.

**Ms GRIERSON**—Yes, but they did not do that until after you presented to us—

**Ms Batman**—No, that was the day after the incident. That was in August.

**Ms GRIERSON**—Yet DIMIA management did not know. Is that what you are saying?

**Mr Woodward**—The person who appeared before the committee was not aware, but what we are saying is that 150 other people—

**Ms GRIERSON**—Okay. Thank you. We have just heard from DOTARS that, as a result of some breaches in their contract and some concerns they would have about the integrity of their information now, they are contemplating changes to their contract. How do you feel now about your contract—that is, outsourcing everything?

**Mr Woodward**—We are at a point where a two-year extension, which was approved in relation to EDS, needs to be considered, because it takes at least 12 to 18 months if you are going to change a contract. We are at the point where we are seriously considering whether we should extend the contract for another two years when it expires, or whether we do not. That is just part of the process where this and all of the other factors—value for money, quality of service, relationships—will be borne in mind. This will not be a sole driver.

**Ms GRIERSON**—All right. Finally, you tell us in your submission that there will be an interim report later this month. Will that be made available to our committee?

**Mr Woodward**—Which interim report?

**Ms GRIERSON**—The submission states:

The Minister for Justice and Customs has also announced an independent review of the Australian Customs Service security procedures, that will provide the Government with an interim report later this month.

**Mr Woodward**—That committee was set up by the government on the recommendation of the minister. There has been an interim report and a draft report forwarded to the minister. There has been no final report. The report is to the minister and it will be for the minister to decide who gets a copy.

**Ms GRIERSON**—Thank you.

**Senator LUNDY**—Just to close off: I ask for the committee and witnesses to consider making the in-confidence submission public. I am looking through it and I am at a bit of a loss to see where—

**Mr Woodward**—Could we reconsider that and, if it is appropriate to downgrade it—and I understand the position—we will do so.

**Senator LUNDY**—I appreciate that, I think we have probably covered a lot of the ground and this just adds to the factual recording of events. I think it would be useful.

**CHAIRMAN**—It goes back to the first thing I had to say when we opened the hearing, and I think that is probably right.

**Mr Woodward**—If at all possible, we will do so.

**CHAIRMAN**—I cannot see anything in that letter that really is in confidence.

**Senator LUNDY**—Finally, a question you obviously heard me asking previous witnesses went to outsourcing contracts. What sanctions are contained in the outsourcing contract that you have with EDS to allow you as a client to penalise or sanction EDS for breaches of IT security?

**Mr Woodward**—In short, I think the answer is the same as others gave you, but I will pass to Mr Harrison.

**Senator LUNDY**—So the answer is: not much except for termination of contract?

**Mr Woodward**—That is my understanding.

**Mr Harrison**—I think there is a fuller answer, but I am conscious of the time constraints. Termination is a sort of capital punishment type response.

**Senator LUNDY**—I put it to you that it is not exactly an effective possible sanction in these kinds of circumstances because of the 18-month process of changeover if it were to become an eventuality.

**Mr Harrison**—If we were to invoke the termination clause, our contract has what I think are adequate transition arrangements. That would be a transition for 12 months after the indication of the termination clause. I think it is realistic in those terms. But I think there are other mechanisms, without invoking that clause, that also help the relationship and enable us to deal with it—and we could talk about that at length. If we talk about the lack of financial sanctions around IT security, those issues are somewhat complex in the sense of responsibility, and the financial sanctions are related to the services that are being provided. You need to look at isolated incidents about who is responsible for what.

**Senator LUNDY**—Can you confirm that no Commonwealth data held or managed by EDS is held offshore?

**Mr Harrison**—I can.

**CHAIRMAN**—Mr Woodward, notwithstanding Senator Lundy's last question and Mr Harrison's answer, you did say to us in writing that the security of that facility was not EDS's responsibility but yours.

**Mr Woodward**—Our physical security is our responsibility. To the extent that the process has failed in relation to the physical security, we are culpable.

**CHAIRMAN**—I just wanted to make sure that that was clear and on the public record. Thank you very much for coming. We await your further answers with anticipation. If we have further questions, you wouldn't mind if we put them in writing, would you?

**Mr Woodward**—No problem.

[12.54 p.m.]

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

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

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

**MACLEOD, Mr Scott Cameron, Team Leader, Computer Network Vulnerability Team, Defence Signals Directorate**

**MCLEOD, Mr Steven Charles, Acting Technical Adviser, Computer Network Vulnerability Team, Defence Signals Directorate**

**MERCHANT, Mr Stephen John, Director, Defence Signals Directorate**

**STROUD, Mr Steven Ronald, Acting Manager, Information Security Policy, Information Security Group. Defence Signals Directorate**

**CHAIRMAN**—Welcome gentlemen. Thank you for coming and thank you for agreeing to sit together. So that we have formal procedures, do not ask each other questions, just answer ours if you do not mind. You have been listening to some of the evidence so you know of the kinds of things we are concerned about. I want to ask a question of the AFP first. In the submission that we got today, you say that you have had 13 laptop computers stolen during the reporting period that I asked for, which was 1998 to date, and that APS, which is a subset, has had one stolen. Did any of those computers contain sensitive information?

**Federal Agent Jamieson**—In the sense of sensitivity some contained operational material, but nothing above highly protected.

**CHAIRMAN**—Operational material that would give those who operated in the underworld or thieves some idea about how you operate?

**Federal Agent Jamieson**—If they were able to access the material, yes it would.

**Senator LUNDY**—What are the grades higher than highly protected?

**Mr Ryles**—Australia runs a two-tiered classification system. National security, which most people seem to be familiar with, has confidential, secret and top-secret levels. Non-national security has in confidence, protected and highly protected levels. Law enforcement tends to come under that.

**Senator LUNDY**—Highly protected is the top of the non-national security ratings?

**Mr Ryles**—That is correct.

**CHAIRMAN**—Does DSD think we need to change that ratings system, or to have a look at that now?

**Mr Merchant**—No, I do not think we need to change the rating system. We would not see that as necessary in the light of information.

**Senator LUNDY**—Going back to the response to the chair's question, does the AFP have any information of a national security nature on their laptops and so forth?

**Mr Ryles**—No.

**Senator LUNDY**—So the point is that it is, as you said, Federal Agent Jamieson, only to highly protected. That is obviously the highest level that you would have access to anyway.

**Federal Agent Jamieson**—Yes, on the laptops, because that is the rating the laptops are given with the encryption software.

**CHAIRMAN**—Does DSD have a view about laptops? We have had one here today that perhaps laptops should be left secured by cable, bolt or other device to the office desk, where they are perhaps normally used, and not taken out of secure premises.

**Mr Merchant**—I think that is unrealistic in this age. Laptops are designed for portable use of computing and IT equipment. I think our view would be that there need to be proper and very tight procedures in place for monitoring the possession of laptops—that is, knowing who has those laptops and that, when they are taken out of secure premises, appropriate certification is provided for their removal and re-entry.

**CHAIRMAN**—Would you think that this inquiry would lead to someone working on a new set of protocols as to what goes on laptops and what can be taken home?

**Mr Merchant**—I think what goes on laptops is consistent with the understanding of the classification level. I think that is firmly in place. In terms of protocols for movement of laptops in and out of government departments, that is an area that could well deserve some more attention.

**CHAIRMAN**—I understand—and I may get some of these details slightly wrong—that a three-star general in England during the first Gulf War took the whole operational plan on his laptop and had it stolen out of his car or a taxi. Does that sound about right?

**Mr Merchant**—Sorry, but I am not familiar with—

**Mr Burmeister**—It sounds like a familiar anecdotal story.

**CHAIRMAN**—We obviously do not have anything comparable—thank goodness!

**Mr Ryles**—I think it happened but it was a Royal Air Force wing commander.

**CHAIRMAN**—Does DSD think that it would be practical to require all Commonwealth laptops to have a removable hard drive that should be carried separately to the machine?

**Ms GRIERSON**—We would be losing a lot of hard drives as well, just in separate—

**Mr Merchant**—That is a valid point.

**CHAIRMAN**—We are supposed to ask difficult questions.

**Mr Merchant**—I am not sure what the cost implications would be if that type of restriction were placed on the laptops. I think the more productive areas to look at would be the stricter control of the movement of laptops in and out of premises, how they are accounted for and whether laptops are actually issued to individuals or to organisational entities. There are greater levels of accountability if laptops are assigned to individuals, and they know that they will be held accountable for the movement of that laptop, rather than assigning it to an organisational entity. Other areas to look at include certification for laptops, particularly laptops carrying sensitive material—certification for their movement outside of appropriate premises—and also regular audits.

**Ms GRIERSON**—Do you think there are enough levels of hierarchy in terms of the controls on laptops that do have high security information on them?

**Mr Merchant**—I think that is an area that would merit further investigation.

**Ms GRIERSON**—I think we would agree with you on that.

**CHAIRMAN**—I see that the AFP has lost 13. From the responses we have received to the letters I wrote requesting information from organisations about loss or theft of hardware, it would seem that, of the items stolen or lost, it is almost always laptops that have been stolen or lost—though we do not have a summary yet because the responses are still coming in. What kind of success rate do you reckon the AFP has in recovering them?

**Federal Agent Jamieson**—I would suggest that, because of their attractive nature and the fact that there is a market out there for such items, it would be very low.

**CHAIRMAN**—I think our submissions indicate that.

**Senator LUNDY**—Further to the security vulnerabilities presented by laptops per se, with the advent of more sophisticated third generation mobile phone devices and PDAs, what advice does DSD offer agencies and departments in the issuing of those types of devices, particularly when many of them now do have the capability to log into databases and agency computer systems?

**Mr Burmeister**—In the end, it is a risk management approach that departments need to take. A general advice, however, is that wireless devices should not be allowed and wireless networks should not be created.

**Senator LUNDY**—Is that because—

**Mr Burmeister**—The inherent insecurity.

**Senator LUNDY**—some of them do not have any encrypted signals, so they could be easily tapped into.

**Mr Burmeister**—Correct. With laptops, obviously it depends on what the equipment is going to be used for. If it is for a purely unclassified role, the normal protections that you would put in place for an attractive asset should be put in place. As Stephen has already mentioned, there should be proper auditing to allow for accountability of that equipment. If it is going to be used for non-national security but protected or highly protected information, we mandate a level of encryption. There is an encryption product that is available on our evaluated product list which I think most people have indicated to you that they have been using to protect the hard drives.

The national security realm is a little different. Obviously there are tighter controls on how the laptops can be moved. Generally at this stage we have some difficulty in providing an appropriate encryption product that would allow classified laptops to be walked out of buildings and taken into non-secured spaces. Those procedures are fairly well laid down.

**Senator LUNDY**—Where?

**Mr Burmeister**—ACSI 33 mentions them to some extent. There are procedures that we would advise individual agencies on if they talked to us. Generally the PSM would hold, even for laptops, as a storage medium.

**Senator LUNDY**—Harking back to earlier evidence that this committee has heard about the reporting system for incidents and IT security breaches managed by DSD ISIDRAS, you might care to remind me what that acronym stands for.

**Mr Burmeister**—Information Security Incident Detection, Reporting and Analysis Scheme. It is a mouthful.

**Senator LUNDY**—In the context of that reporting scheme, which has been in place for some time—and I know DSD has been working hard to promote it amongst agencies and departments—the chair has asked agencies and departments to respond to breaches of IT security. We have been given that documentation today and it is being published for the first time today. I would like you to research that information and report back to the committee on how many of the items that we have now been informed of were advised to DSD through the ISIDRAS system. I think it would be extremely useful for this committee to get a feel for it—to reconcile what you are hearing and learning about and are therefore in the position to develop policies in response—and what has been occurring in agencies and departments over the years.

**Mr Burmeister**—We can do that, although my off-the-cuff remark would be that very few of the historical incidents that have been reported to you over the four- or five-year period would have been reported to us.

**Senator LUNDY**—Could you indicate in your response the points at which DSD undertook to raise awareness in the ISIDRAS reporting program and how that shows how incidents have been, hopefully, reported on a more common or regular basis?

**CHAIRMAN**—As soon as each one is authorised for publication, we will make them available to you. I cannot do it before that.

**Mr Merchant**—Do you want that done over the full five years?

**Senator LUNDY**—Yes.

**Ms GRIERSON**—Do you want to know whether it was reported to AFP and DSD?

**Senator LUNDY**—No, just to ISIDRAS. I now turn to the Customs incident. Was that reported to ISIDRAS?

**Mr Merchant**—The Customs incident?

**Senator LUNDY**—The theft of the servers.

**Mr Merchant**—Yes, it was reported.

**Senator LUNDY**—We discovered today that two more PCs were stolen at the same time. Was that ever reported to ISIDRAS?

**Mr Merchant**—Not to my knowledge.

**Mr Burmeister**—Not formally. We had some informal knowledge. Did it start off as two CPUs or two desktops?

**Mr Stroud**—Two CPUs and a battery pack.

**Mr Burmeister**—That was reported to us a couple of days ago. —not so much reported; we were informed in the course of comment on a submission that was going to the Minister for Justice and Customs.

**Senator LUNDY**—In the context of the information this committee has received, what we have heard today—and contained in one of the reports published—was that there were two additional pieces of computing equipment. We now know that to be two desktops and a battery charger.

**Mr Burmeister**—Today was the first we had heard about it.

**Senator LUNDY**—When you say you informally heard about it a couple of days ago in the context of, presumably, these submissions going to the minister or perhaps the Attorney-General's submission to this committee, was that the first time you had become aware of it?

**Mr Burmeister**—Yes—that there was equipment in addition to the two servers that we knew about.

**Senator LUNDY**—So you have not been officially advised through ISIDRAS about the theft.

**Mr Burmeister**—Not to my knowledge.

**Senator LUNDY**—What would the process normally be for you to be advised?

**Mr Burmeister**—I would have to say at this point that ISIDRAS is still a work in progress. We are still working a lot on our education programs and getting the agencies and departments aware that ISIDRAS exists as a formal reporting mechanism. For the purposes of ISIDRAS, we would consider physical loss of equipment to be probably a level 3 incident. So it really is a mandatory reportable incident—and a number of people have been surprised when we have said that. In terms of the DOTARS incident, for example—I think you mentioned it was 22 August or thereabouts—

**Senator LUNDY**—That is correct.

**Mr Burmeister**—We actually contacted them—and I think DOTARS mentioned it themselves—on the basis of the reporting in the press, and they subsequently put in an incident response. They had not approached us independently before that. I have to say that we do actually have a fairly proactive line with incident reporting. If we hear about something and a department has not told us, we will go and seek a report. Often it turns out that they are not aware of the scheme—which is one of the things that we are trying to improve. If they are aware of the scheme they are not necessarily aware of what each of the levels means and which incidents they need to report to us.

**Senator LUNDY**—Could I confirm again that ISIDRAS represents the only whole-of-government reporting scheme for IT security incidences and potential breaches?

**Mr Burmeister**—That would probably be a fair statement.

**Senator LUNDY**—So the government has no way of knowing what is going on in this area, unless you tell them—from a holistic perspective.

**Mr Burmeister**—That would probably be fair, yes.

**Senator LUNDY**—Thank you. With regard to DSD's advisory role, I want to refer back to comments made by DSD in the context of the whole-of-government information technology infrastructure outsourcing. DSD advised the audit office at the time:

> A conclusion to be drawn from the DSD experience and also from the report, is that given the present state of the industry in Australia, outsourcing the management of high security networks would be a risky and also costly business. External service providers are not experienced in managing networks to national security standards, as commercial risk drivers do not equate readily to government accountability requirements, let alone to managing counterintelligence threats. The identification and then oversight of contractual obligations would therefore be even more resource-intensive than for conventional government networks.

Then you go on to make another point about it being core management. The finding—and DSD suggested at the time—was that agencies create and maintain an enterprise security architecture document. Can you tell the committee whether or not that recommendation by DSD, at the time when the security aspects of these three major outsourcing contracts were considered, has been

followed through in any way—either by those agencies or by any other agency or department? I think you identified these issues and problems back in the year 2000.

**Mr Burmeister**—There are two aspects to this. The comment that you read out was in relation to national security networks. To my knowledge, nobody has seriously considered outsourcing a national security network. DSD, as part of the Department of Defence, has always said that, whatever the department does for its broad IT outsourcing considerations, if it decides to market test, we would prefer that DSD's networks not be part of that. I think that has been broadly accepted.

**Mr Merchant**—Absolutely.

**Mr Burmeister**—In terms of enterprise security documents—or whatever the phrase was—

**Senator LUNDY**—Enterprise security architecture document.

**Mr Burmeister**—Right. When we work with departments to give advice on how they should set up IT infrastructure, there is a general set of documents that they ought to produce that we would then review. That includes security plans, architectural and network diagrams—things that we can help them develop. Whether or not a document of that type exists, there are certainly a number of documents that we would expect every agency to have so that they completely understand the nature of their networks.

**Senator LUNDY**—Do you think they have that documentation?

**Mr Burmeister**—If you were to look at some of the other ANAO reports that came out subsequently, I think you would probably find that the answer is no.

**Senator LUNDY**—Yes. I was going to go to that one next.

**Mr Burmeister**—When we do work with agencies and do security audits with them, our experience is that often documentation is not complete or it is out of date. So there is not a single standard yet for the documentation that agencies should have to be able to understand what the networks are.

**Senator LUNDY**—There is no overarching mandatory standard for IT security in the Commonwealth government either, is there?

**Mr Burmeister**—Not mandatory, no.

**Senator LUNDY**—How many departments and agencies are you aware of that do choose to implement both ACSI 33 and the PSM as mandatory in their minimum standards?

**Mr Burmeister**—I am not sure I could give an answer to that. Certainly the larger departments would, and those that have a national security focus certainly would. I would think that, generally speaking, most agencies, including the smaller ones, would try to implement those that make sense within their contexts and within their overall risk management arrangements.

**Senator LUNDY**—After the evidence we have had this morning about the added complexity that having IT outsourced introduces, how confident is DSD that when incidents do occur they are actually being reported, to the agency, to the department, to the appropriate authorities like the AFP or, indeed, through ISIDRAS?

**Mr Merchant**—It is hard for us to speculate. We do not know what we do not know.

**Senator LUNDY**—What are your suspicions? Do you think it is worse than what you know of?

**Mr Merchant**—As I think Tim has said, we would like to raise the profile of ISIDRAS.

**Senator LUNDY**—You obviously think that is necessary.

**Mr Merchant**—We have been trying to do it so we obviously think it is necessary. We do not have the resources to put people onto unnecessary tasks. I would like to be able to throw more people onto that type of effort and to promote the role that DSD can play in response to incidents that compromise or potentially might compromise government security information networks.

**CHAIRMAN**—We could probably do a good job of that for you.

**Mr Merchant**—I agree, and I think that is one of the values of this inquiry.

**Ms GRIERSON**—Having listened to today's evidence, there is a real problem in that departments say to us in their submissions and in their responses that their security responsibility is the physical security where those assets might be placed. However, when assets are stolen and they are part of an outsourced contract, the information flows are absolutely confused, the lines of responsibility are confused, and their knowledge of those assets and I think their handling of the levels of information have been revealed as being not satisfactory. So it does seem that risk management processes do have to really deal with who is responsible for what and who tells whom. There are things you cannot devolve to a contractor, yet it seems there is some complacency by departments and that they do devolve some security responsibilities to contractors that perhaps are not being enforced, audited or monitored. I would like you to comment on that and perhaps suggest ways that can be improved.

**Mr Merchant**—We would be very happy to work with government departments in advising them on the construction of contracts for outsourcing of IT. Again, as a result of some of the discussion this morning, that could impose very heavy demands on DSD, but we do have quite a value-adding role to play in that regard.

**Ms GRIERSON**—DOTARS have suggested that there are some functions of their IT that they now think should not be outsourced. Would you have a view on that?

**Mr Burmeister**—I would say that the DOTARS experience replicates the experience of other agencies that have had similar occasions to deal with.

**Ms GRIERSON**—In this new heightened national security environment, they could change.

**Mr Burmeister**—Certainly. But I would have to say also that it is something that has been brewing for some time, possibly even before September 11.

**CHAIRMAN**—When you talk about added workload and you talk about resources, if we make recommendations that involve you, you are going to ask us to also make recommendations for the resources to do the work. Is that right?

**Mr Merchant**—I am concerned that I can see a lot of work flowing to DSD as a result of this committee's inquiry, which has both good and bad points to it.

**Ms GRIERSON**—I have a last question for DSD. What are the security implications of having encryption software, encryption modems and that sort of material going missing or being misplaced? Can you use those to reverse the process and analyse the process.

**Mr Merchant**—It depends on the circumstances of the case, of course.

**Ms GRIERSON**—So you would be reviewing some of those incidents that have been brought to our attention?

**Mr Merchant**—We have not seen the submissions.

**Ms GRIERSON**—We only got them today.

**Mr Merchant**—I was interested to hear from the Customs officers that were here before us about the incident and our involvement in that. We do not have a full brief on that today, but our understanding is that we were involved in that investigation. It involved commercially available encryption. It was not encryption protecting national security classified material—around which there is a very strict set of procedures—which DSD, particularly for the highly protected stuff, is very concerned to protect. I am not sure, Tim, whether you can add anything more about our action on that particular incident.

**Mr Burmeister**—The two modems that you mentioned are likely to also be commercial cryptography. They would have been used to carry sensitive information but not national security information. There is a whole different regime—

**Ms GRIERSON**—And they would have been provided by a contractor rather than their system?

**Mr Burmeister**—The department might have bought them, but they would not have been provided by us. There is a whole different regime for what we term 'high-grade cryptography'.

**CHAIRMAN**—I must admit that I am pleased that we have so far not discovered any incident like the one in England with the whole war plan on a laptop. That does give me some confidence.

**Senator LUNDY**—I would like to ask the AFP a question about resources. As these incidents are on the rise, how capable is the AFP of responding to and pursuing specific inquiries in

relation to all of these incidents that are occurring within Commonwealth agencies and departments alone?

**Federal Agent Jamieson**—That is a very difficult question to answer because, as you are aware, we do not actually get reports of all incidents to us. But every incident that is reported to us is assessed appropriately in conjunction with the reporting agency. We make an assessment both on the loss of the asset as well as on the possible damage from the data—for example, if we are talking about laptops. In that context, it is very difficult to give any definitive response.

**Senator LUNDY**—What about the example where Customs and EDS chose not to report to the AFP the theft of two PCs from Link Road in Mascot? To me that looks like a very high level of negligence and irresponsible behaviour. What is the AFP's take on the fact that people choose not to report theft?

**Federal Agent Jamieson**—I suppose we take the view from the Commonwealth policy on fraud control. Essentially, it is a CEO's responsibility to report the matters to the appropriate authorities to undertake the investigation.

**Senator LUNDY**—Is there any mandatory obligation for them to do that?

**Federal Agent Jamieson**—No, there is not.

**Senator LUNDY**—So it is a discretionary issue?

**Federal Agent Jamieson**—Correct.

**CHAIRMAN**—Thank you for coming and talking to us. I thank my colleagues and the secretariat staff—and, as always, God bless Hansard.

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

That this committee authorises publication of the proof transcript of the evidence given before it at public hearing this day.

**Committee adjourned at 1.23 p.m.**