LEGISLATIVE ASSEMBLY FOR THE AUSTRALIAN CAPITAL TERRITORY

STANDING COMMITTEE ON ADMINISTRATION AND PROCEDURE

(Reference: the role of InTACT as the Legislative Assembly's service provider)

Members:

MR SPEAKER (The Presiding Member)
MS R DUNDAS
MRS V DUNNE
MR J HARGREAVES

TRANSCRIPT OF EVIDENCE

CANBERRA

WEDNESDAY, 10 SEPTEMBER 2003

Secretary to the committee:
Ms J Rafferty (Ph: 6205 0557)

By authority of the Legislative Assembly for the Australian Capital Territory

Submissions, answers to questions on notice and other documents relevant to this inquiry which have been authorised for publication by the committee may be obtained from the committee office of the Legislative Assembly (Ph: 6205 0127).

The committee met at 9.34 am.

MICHAEL VANDERHEIDE,

ERNEST HOCKING,

RICHARD HART and

IAN WATERS

were called.

MR SPEAKER: I declare open these proceedings of the Standing Committee on Administration and Procedure and welcome members Mr Hargreaves and Ms Dundas. This is our first public hearing on the role of InTACT as the Legislative Assembly's service provider. I welcome witnesses from InTACT.

Before we proceed I would just like to go through some formalities. You should understand that these proceedings are legal proceedings of the Legislative Assembly protected by parliamentary privilege. That gives you certain protections but also certain responsibilities. It means you are protected from certain legal action such as being sued for defamation for what you say at this public hearing. It also means that you have a responsibility to tell the committee the truth. Giving false or misleading evidence will be treated by the Assembly as a serious matter.

The other thing I might mention at the outset is if we are tending to traverse onto grounds that might go to security issues, it is open to you to request the committee to go into camera so that you can give evidence to the committee in camera and we can treat it confidentially. That is subject, of course, to committee members agreeing to an approach along those lines.

With those issues out of the way, would you like to make some opening statements about InTACT's position in relation to this inquiry?

Mr Vanderheide: I am Michael Vanderheide, general manager of InTACT. Thank you very much for the opportunity to be here today. I might just start by introducing some key members of my team that I have brought with me. Ernest Hocking is the director of service delivery, which means that he is responsible for the help desk, onsite support and customer service level agreements; Richard Hart is the director of solutions delivery, which is basically the engine room of InTACT, with all of the stuff that blinks and whirrs in the background; and Ian Waters is the acting manager of security. My security manager is on his honeymoon at the moment or he would have been here as well.

I thought I might just say a couple of words about what InTACT does, because sometimes the boundaries between InTACT and other bits of IT across the organisation are a bit unclear. We were formed in 1996. I have been told by a number of people that it was quite a difficult birth, in the sense that it was a forced centralisation of what had been a decentralised IT support model. What that resulted in back then was an organisation that had lots of people in it who really did not necessarily want to be there supporting an IT environment that was eclectic at best. We had 20 different word processing systems and email systems within government that meant that we were unable to send emails to each other. It was a bit of a mess.

It was also set up with the view that within a year's time or so it would be outsourced, and that the ACT government, like the federal government at the time, would source its IT services from an external organisation, which could have been InTACT but could have been somebody else. Given the experience of the federal government's outsourcing, we are probably pleased that that did not come to pass.

We invested heavily in IT just before the year 2000, in what was called the modernisation project, and we continue to reap the benefits of that investment today, with a single government network, a common operating environment across government, procurement that is quite centralised and lots of things that serve the government well.

We are basically the IT infrastructure providers, and that means that we are responsible for everything from the desktop back. We do PCs, printers, faxes, scanners, telephones, mobile phones, the networks that connect all these things up, the boxes and the servers that sit at the other end with the business applications. We are a bit like Actew in the sense that we provide the wires and the equipment that provides people with the ability to do their work.

Agencies have responsibility for business applications, which are the applications that sit on our infrastructure, and then there is a separate organisation called ACT Information Management in the Chief Minister's Department that has responsibility for establishing policy for IT across government in both. They do that with a view to what is best for government as a whole as opposed to what is best for individual agencies or for InTACT. We all work together to develop those policies.

We are here today because about a year and a half ago a minister's email was redirected and that was a significant blow to our credibility and to the image we have of ourselves as a professional organisation. More importantly, though, it was, as we said in our submission to this committee, a breach of trust of the highest possible order and, on behalf of my organisation, I apologise for that breach having occurred.

It would be fair to say at the time that our security efforts were more focused on protecting ACT government networks from external threats as opposed to dealing with what could go wrong inside the organisation, and we have taken a lot of steps since that time to ensure that our security is up to scratch. My guess is that we will be talking a little about that this morning and I appreciate the opportunity to go in camera if we need to.

We are representing an organisation that takes pride in what it does. We take pride in the services we offer; we take pride in the work that we do. We also know that there are a lot of things that we need to do better, and we are working very hard to do better at those things. That is probably all I wanted to say to start.

MR SPEAKER: Thank you very much for those comments. Noting your comments about the inquiry into the unauthorised diversion and receipt of a member's emails, which was the genesis for this inquiry, the committee's report was highly critical of

InTACT and used very strong language such as: “The whole process reflects very badly on InTACT.” I do not want to keep reminding you of these things because I am sure it is a recurring nightmare.

Mr Vanderheide: Yes, it is.

MR SPEAKER: We all have to move on and we are hopeful that, as a result of this inquiry, we are able to move on in a productive and positive way. I would like to hear some of the details of how you have responded to the criticism that was levelled at you by that inquiry report. Would you be able to give us some evidence along those lines?

Mr Vanderheide: Absolutely. What I would be very happy to do is to tell you what I feel I can talk about in a public way. If you are looking for more detail, I will certainly be able to give you that, but we may have to go in camera. There is a whole range of things in response to that. It was not that we did not have security at the time—we certainly did—but, as I said, it was focused largely at protecting the organisation from external threats.

Immediately following the incident we began to implement better security arrangements within InTACT and within government. For example, at the time of the incident we had over 80 staff with the appropriate levels of privilege to get in and make the changes that were made in redirecting email. Now, just over 20 staff have that privilege. In addition to that, all of those staff are subject to a security vet to either a protected or a highly protected level. That is the case across a number of positions across InTACT, I and others around me included. We are recognised as running something that is pretty close to best practice across government in the security vetting process.

There is a high level of security awareness across InTACT and that now permeates everything we do. At the time of the incident we had one individual who had responsibility for security. She was relatively lowly placed in the organisation and we have shifted from that to having five individuals now forming a security team. That security team reports directly to me, both to ensure that it gets the appropriate profile and that there can be no perceived interference, I guess, by operational demands on the work that they do.

The quality of staff we have on that security team is also quite considerable. The individual who is running it has been recruited from his role as security manager in the federal department of health and Ian comes from the Defence Signals Directorate. There are three other staff more junior than that working on security as well.

We are accountable for all things related to IT within government. There is a three-level government structure: a DIO group, departmental information officer group, at the operational level; a CIO group at the strategic level; and then on a monthly basis we report to something called the information management board which is a forum that is chaired by Rob Tonkin and comprises all of the chief executives across government. On a monthly basis we provide a security update as to progress on projects that we have under way associated with security, so the level of interest in this is obviously very high as well.

From a technical perspective we have put in place the logging necessary so that, should an incident similar to what happened with Minister Wood's email happen again today, we would be in a position to tell you who did it, when it happened and how it happened. Probably more importantly than that, we are also proactively monitoring the delegation set-ups within the Assembly in particular to ensure that nothing unusual is happening. If we spotted something unusual, we would be in touch very quickly to ask if it was intended. If so, that is great; if not, we would need to do something about that. We also continue to proactively manage the potential for external threats.

Finally, we are focused very much on user education. We circulated a brochure on general IT security to all ACT government staff. I do not think it has been circulated within the Assembly or to Assembly staffers at this stage, but it certainly can be. There is an expectation that there will be an ongoing program of security education both within InTACT and for our customers because it is a shared responsibility in a big way.

MR SPEAKER: I will consult with my colleagues on this, but I wonder whether it might be useful for us to deal with what might be confidential issues around security early in the piece. Would that be useful for you?

Mr Vanderheide: It really depends what you want to know. We are happy to go into more detail on any of those things.

MS DUNDAS: I have two questions relating to security. I am not sure if they need to be in confidence.

MR SPEAKER: Okay. At any point if you think something that we ask is a security matter we can put that one aside. If we get a little group of issues that need to be dealt with in camera, we might deal with then that way. Is that okay, members?

MRS DUNNE: That sounds like a good idea.

MR SPEAKER: Another question I would like you to address is how you deal now with the separation of powers between the executive and the Assembly in your security processes?

Mr Vanderheide: Not very extensively, I have to say. To a large extent work around that has been waiting for the outcome of this meeting. We have done some work. We've certainly been speaking to Val extensively over the past few months as to what the opportunities might be. Even before the email incident some work had been done as to what could be done to separate the Assembly's and the executive's arms.

MR SPEAKER: That is part of the options that you've got in your paper?

Mr Vanderheide: It is. We are in the process of separating the disk volumes the data for the Assembly is stored onto to ensure that there is clear separation between the executive, the Assembly, the members of the secretariat. To some extent we can do just about anything you want us to do. We just need to know what you want us to do. We've provided some options in our paper and I understand that you've got a couple of other options as well. We could mix and match between those in a few different ways. There are probably other things we could do. We need to know what the need is.

MR SPEAKER: Do members have any questions?

MS DUNDAS: I understand that at the time the privileges report was tabled—I could be wrong about this—the Chief Minister announced that he was going to do an internal review. Has that review been completed and if so is there a report that we could see to give some of that greater evidence about how changes have been made?

Mr Vanderheide: I think that you can see it, but the report was actually commissioned by the Chief Minister's Department. So we have it, but we do not have it to give, but the Chief Minister's Department organised an internal audit for us.

MRS DUNNE: In that case the Chairman might have to write to the Chief Minister.

MR SPEAKER: Can we put that down as a decision we have to make—to call for papers? We can deal with that later if you like.

MS DUNDAS: But you're briefly touching in your submissions some of the outcomes from the upgrades you've made and you've briefly touched on them today. Specifically in one area, security audits, how do you go about conducting those.

Mr Vanderheide: We have our own program of internal audits within InTACT that we run on a security basis to ensure compliance with our own procedures and policy. Ian might be able to talk you through that.

Mr Waters: Our main purpose is to make sure that the logging in place to prevent another occurrence of the email incident is actually in place and working, and that the log's been collected and so on.

MS DUNDAS: Can I just jump in at that point. There is a lot of focus on the issue that occurred and how to prevent that, but is there also greater focus on all the other things that can go wrong with email?

Mr Waters: Yes, certainly there are. That is just part of it. With that a whole gamut of logging is occurring at all times. We audit that that logging is occurring and that the logs are being stored safely and are being kept in a secure manner so that there can be no interference with them. They're actually burnt to CDs and they're locked away. So we can be fairly confident that if there is another security incident of any sort we are able to resurrect and work out how it was done, by whom and when.

MS DUNDAS: That is the ability to find out what happened at the end. As preventative measures you've reduced the number of people who can actually have access to the system?

Mr Waters: Yes.

MS DUNDAS: What else is happening there?

Mr Hart: We are also running an internal audit program which, in some cases, consists of our own people doing the work and in other cases engaging outside assistance to undertake management audits; in some cases helping us to better understand the issues around a particular aspect of security and how we may structure ourselves appropriately to deal with that; and in some cases compliance audits to determine to what extent we are complying with our own internal policy and whether there are any improvements that need to be made there. We've done that, for example, in relation to management of administrative permissions—the sort of thing that tripped us up with the email diversion. We are very conscious that an overall enhancement of security means that we can't be focused on fighting the last war, we can't be focused on just dealing with the specifics of what happened in the email incident.

MS DUNDAS: When we had the incident a couple of weeks ago when the virus went around, my computer was continually being updated with patches to the point that I just walked away from it at some point. That was happening across the ACT government network. How is the number of people who have security clearance to access the Assembly network being monitored? If you had an increasing workload, did you have a specific team just doing the Assembly computers?

Mr Hocking: Within InTACT we have a very clearly defined security incident process and procedure. That was effectively initiated and implemented as a result of that particular virus incident we experienced. That requires that we form a team that actively manages the incident from start to finish. That deals with doing an analysis of the problem, dealing with the escalation to make sure that people like Michael as the general manager and, if necessary, other parts of government are informed of what is going on, as well as dealing with the technical issue. By bringing that team together very early in the process we can manage that right from start to finish.

If something like the ministerial incident occurred in the future, we would implement that exact same security incident process and manage it in a much more effective way than perhaps happened in the past, when essentially a very junior individual was tasked with all of those security issues.

MS DUNDAS: So that team being set up to manage the virus hit, would have included people obviously authorised in terms of the Assembly?

Mr Hocking: Absolutely. If I just think through who was there, all the people involved in that particular incident had had a vetting. In that particular case not everyone had been vetted to the level of highly protected. If I may interpret your question about what would happen in an incident within the Assembly—

MS DUNDAS: Well, just how you manage the Assembly as part of the whole-of-government network, as this was a problem that hit the whole of government?

Mr Hart: That blaster worm is a good example of how we act now. At a very early stage we declared a security incident—about 4.11 in the afternoon on that day. The first step was identifying who needed to be involved, getting those people together and discussing how we needed to both technically attack the issue and how to communicate what our communication strategy would be internally within the organisation and at our client agencies.

At about 5.15, I think it was, we held a meeting of those people. Included in that were the heads of service teams—what we call our hosts for each of the main customer groupings. The head of service team for the Legislative Assembly was involved in that. We established a plan for how the hosts would communicate with the departmental information officers; what, if any, direct communication to individual officers was needed; and how we would in an ongoing sense monitor and manage our performance during that incident.

So at a very early stage we considered the issues of our clients via the structure that we currently have to manage our relationship with those clients. In that sort of incident it is our experience that it is best to use the structures that you have day to day because they're most likely to work for you during the incident.

MS DUNDAS: There are recommendations in this of building a greater logical separation between the Assembly network—network's the wrong word, but you know what I mean—and the rest of the ACT government. If another incident arose—I am talking more about viruses than security breaches at this point—where you have a problem across the entire network, how would the logical separation or a greater logical separation either hinder or help you in dealing with that virus across the network?

Mr Hocking: I will make a comment on that. When we talk about a logical separation in the context of the proposals and the options that have been put forward, that would only just be one of a number of measures. As in any organisation, InTACT is constantly reviewing a number of different aspects of the way that it operates. One of those, for example, is the telecommunications area, and Richard might make comment on that later. But within the telecommunications network itself we can achieve some separation, which would have the effect of reducing the impact of some of those virus-type attacks.

In addition, we would take additional measures that would, for example, require the use of different service, physical pieces of equipment, to separate the Assembly from the rest of the government. We would then apply this logical separation that is referred to in the submissions along the lines of organisational units. So it is unlikely that a single measure would meet all the requirements that we believe would exist in the Assembly.

Mr Vanderheide: Are you concerned, Ms Dundas, that if we have this kind of separation the Assembly may not have the support that it would otherwise have?

MS DUNDAS: Not so much that it wouldn't have the support, but when you're working with an entire system it is easy—using layman's terms—to use one big patch and fix it all at once. If you start separating different units you then have to do one big patch and another patch here, and that might come second because you're trying to deal with the hospital's computer systems or the Department of Urban Service's computer systems immediately. That would then impact on our day-to-day operations.

Mr Hart: If I can perhaps speak to aspects of the technical design. The technical design that we are proposing would still involve, if you like, a last resort overall management control. So, for example, if we had to push a patch out to every workstation in government quickly, we could. That ability would be reserved to a very small number of individuals centrally within InTACT and the extent of that ability would be known to the Assembly departmental information officer. That power would be used reasonably rarely. It would be used basically for that purpose by a small number of closely monitored individuals.

It is a corollary in security that the more power you give to an individual the more closely you watch them. It would be a small number of highly qualified and fairly closely watched people in our central service facilities area. But the design would still reserve the right to apply whole-of-government patches while giving the Assembly a degree of assurance that the routine, the day to day, was only being done by them.

Mr Hocking: Maybe I can expand on that a little bit. One of the things that we did from start to finish during that virus incident was to liase very closely with each of the distinct agencies. Your question about the way we dealt with the hospital, as opposed to other agencies, is a case in point. As a result of that liaison we did time some of the things in different ways. For example, if you had a concern that you had a late-night meeting and in some way we couldn't take action because of an operational requirement that you had, we could arrange the timings to be slightly more suitable in some cases like that, yes.

MR SPEAKER: I am completely lost on the acronyms. I had a quick look this morning at the large dictionary of them in the vain hope that I might remember some of them. From your submission and from what you've said this morning, viruses are treated in the same way as a breach of security by a similar team. Am I correct in saying that team has grown from one to many now?

Mr Hart: It has grown from one to five. There are many viruses. Viruses are only treated as a security incident where they cause a problem. The vast bulk of viruses do not. The blaster variant that hit us a few weeks ago was unusual in that it was released in the Asia-Pacific area first and as a result the anti-virus software vendors hadn't had a chance to develop their patch for it. They're US based by and large and it takes time. The Asia-Pacific area is usually the beneficiary of several hours worth of delay. So we get many viruses and the vast bulk of them do not cause a problem because our automated systems are up to them.

MR SPEAKER: The ones that do are treated as a breach of security of some sort, essentially?

Mr Vanderheide: We treat it as a security incident.

Mr Hart: Until we know otherwise we treat it as a security incident.

Mr Vanderheide: It has grown from one to a team of five, but it is not that there are just five people who work on the problem. That is the advantage of having the resources we've got. We bring in anybody who needs to be brought in to solve the problem.

MR SPEAKER: And you've got to touch base with the relevant people in the agencies as well?

Mr Vanderheide: Absolutely. Absolutely, yes.

MR SPEAKER: I suspect the committee will need to be satisfied that there is a clear improvement on what occurred before the criticism of the committee which said so many rough things about your organisation. That security group is a central part of the changes—the growth from one relatively junior officer to five in the central office of your organisation. Is it also true to say that stronger links have been established between that group of five and the relevant agency contact points? How does that work?

Mr Hocking: Can I make comment on that? Mike made reference to this hierarchy of management groups. At the lowest level, departmental information officers come together on a periodic basis in a group called the information services group. They're essentially co-ordinating things across the whole of government. At the CIO level there is another group called the information management consultative committee, and at the chief executive level the group's called the information management board. What we've done within InTACT is to take this information about what we do on security initiatives to all of those three groups. We brief them on a regular basis about what progress we are making and they have the opportunity to question us and make suggestions about it at the same time.

In addition to those three groups, another group called the IT security focus group meets less frequently. Again, that is individuals from the agencies that come together and at that particular forum the focus is very much on security and issues that affect the whole of government as well as the InTACT IT discussed at that interview.

Mr Vanderheide: The IT security policy is set by ACTIM. It is important to understand that. It is a central policy, ACTIM is the group that runs the IT security forum. The fact that we've got more people doing security has allowed us also to be more proactive in dealing with the agencies so my security team is involved, I think almost without exception, when a new security system is introduced. They're involved in all projects within InTACT, being part of the sign off for the change management process. Having the resources has meant that we could do more than we could do before and the agencies are asking for that assistance.

MR SPEAKER: Have we got an Assembly person in that mix of people?

MS DUNDAS: Can I ask for an organisational chart? If you do have one done up it might identify the different teams and it might make things easy to have a visual representation of what you're talking about and how it is broken down.

Mr Vanderheide: Yes, absolutely.

MR SPEAKER: Let's have a little hypothetical for a moment. In the event that this committee decides to recommend one order or another of quarantining of Assembly IT, can you satisfy us that the person who would represent the committee in this forum, or in your forum, would have sufficient support of the entire group to ensure that security issues do not affect us and give us the same sort of standing that any other agency would enjoy?

Mr Hocking: I think we can probably go further than that, in the sense that at the moment we look at each and every agency's requirements on a case-by-case basis. For example, the Justice and Community Safety portfolio has elements that have very high requirements for security, case in point being the DPP's department. In that area we do expend extra effort to ensure that their security requirements are met. So, rather than say we would provide a consistent service—yes, it is consistent in the sense it is a high level of service—where the Assembly or the executive has different security requirements, we would work very closely with you to meet those specific needs.

Mr Vanderheide: Are you concerned, Mr Berry, that if we opt for this model, the Assembly may be treated to some extent as separate or second-class?

MR SPEAKER: I just want to get the record straight on all of these issues so that the committee is properly informed about where we might be headed with whatever decision we come to in the light of the recommendations that are going to be put to us throughout this inquiry.

Mr Vanderheide: Okay.

MR HARGREAVES: Mr Chairman, I would just like to make the point that whilst we depend very heavily on our interaction with the bureaucracy and the systems that they have, and we depend very heavily on the speed of response as well, nonetheless, as the Speaker alluded to earlier, there is a separation of powers issue. It has concerned me for some time that the same level of security applies to my office as would apply to an ASO2 in the department of education. I wanted to be absolutely certain that that was not going to be the case henceforth. That is when we were talking about having firewalls between us and the bureaucracy, or having a separate system and all the rest of it.

I acknowledge it is a really difficult issue, but we need to be able to talk to the ASO2s in education, and we need to be able to talk to them securely. By the same token, we need to make sure that the information that we are sharing with these people is controllable by the Parliament and not by the executive, or by the bureaucracy at large. That is going to be the nub of it for me.

MR SPEAKER: Isn't there an issue of government policy too, about whether or not they want you to talk to an ASO2?

MR HARGREAVES: Those government policies seem to change somewhat when you have more free governments in power than others, Mr Speaker.

MRS DUNNE: Having come out of the Commonwealth to work in this building as a member of staff, and that was admittedly just after InTACT was established, I was stunned by the lack of security. I had come out of a Commonwealth agency where it was a breachable offence to share your password with anyone. I walked into an office where passwords were sort of passed around—I mean it was within an office of people who worked discreetly and closely together.

MR SPEAKER: How did you get to remember them, if you couldn't share them?

MRS DUNNE: It was a case of I need such-and-such, and it is on somebody's machine, you just typed in their password and you got it. We were all ostensibly singing from the one hymn sheet, and all working for the one end in a political office, but having had that sense of security inculcated in me, coming from a Commonwealth department, I was pretty stunned by it, and it doesn't seem to have changed very much. We still haven't got to the bottom of what happened in the last war—and I take the point that you made, Mr Hart, that we shouldn't be fighting the last war—but we still really do not know what happened. So we do not really even have the Guns of August.

Mr Hart: Yes, we do know what happened, Mrs Dunne. We do not know who did it, when they did it or why.

MRS DUNNE: We do not know who did what to whom and why. Yes, okay. So we only know partly what happened. It also struck me—and correct me if I am wrong—that most other parliaments, whilst being part of a government network, are sort of separate from that government network in a way that we are not. That may be a convenience of size.

Mr Hart: They are. In response to the letter from the committee, we conducted a survey of state and territory jurisdictions. There is no one model.

MRS DUNNE: There is no one model, yes.

Mr Hart: The model in the Northern Territory, for example, is very similar to the model employed in the ACT, with the exception that the department responsible for providing IT services outsources components, selected components. South Australia runs a broadly similar model as well, but in the case of the older jurisdictions, usually a department provides IT services, and that is separate in most technical respects to the standard government network. Government policies on password sharing and so forth within government are reasonably strongly enforced. Those policies do not have jurisdiction within this building.

MRS DUNNE: So they are strongly enforced elsewhere?

Mr Hart: Those sorts of things are dealt with administratively within agencies, and certainly dealt with administratively within InTACT. InTACT doesn't have a policing role within an individual department to say, if you've got a password up on a sticky note on the screen, InTACT's going to frogmarch you out.

MRS DUNNE: But that is really a departmental issue. I understand that.

Mr Hart: My understanding is that individual agencies do take quite a dim view of that, but, as I said, those policies do not have jurisdiction in this building.

MRS DUNNE: Okay. All right.

MS DUNDAS: From maybe the end of last year or the beginning of this year, the warning was flashing up every time somebody logged in saying, "Do not use this computer for inappropriate use, your work is being monitored." That was a concern to some members of the Assembly because we do have to use our computers for inappropriate use—checking out web sites as part of our constituent work. I do not enjoy that part of it, but it has happened a number of times. It also raises concerns about how the Assembly's use of those computers was being monitored, and the rules that the government might apply to its staff applying to members who are, to a certain extent, working under a different set of rules. How is that now being managed?

Mr Waters: Could I just answer that? In the security area where I work, we sometimes have to investigate some inappropriate behaviour by some member in a department. We have to actually investigate some of these not terribly nice web sites, for example. However, that is considered to be part of our job, and therefore we are not using it inappropriately, and that is taken to be the case.

MS DUNDAS: Sure, okay.

Mr Waters: I think that the same sort of rules would pertain to people in the LA as well.

Mr Hart: However, Ms Dundas, I think you've touched on an important point, in that InTACT is potentially custodian of information about how MLAs use their systems. The way that information is dealt with needs to be clearly agreed and understood among the parties. One of the things that we are suggesting in our submission is that we need to elaborate in some detail a protocol for how those sorts of things are handled. The convention we've adopted to this date is that we work under the direction and instruction of the clerk of the Assembly. That is fine, but how do we handle whatever information we come across in investigating a security breach in an MLA's office?

MR SPEAKER: There is an acronym for that, isn't there?

Mr Hart: Almost certainly, Mr Chairman.

MR SPEAKER: An SLA. We've got to have an SLA.

Mr Hart: I think that SLA needs to be a little bit more detailed than it does with line government agencies, in some of respects, in how we deal with that. The information needs to be gathered for the efficient operation of the network, but I think that MLAs would be reasonable in their expectation that their people know how that information is being dealt with and have a degree of trust that it is being dealt with according to agreed practice.

MR HARGREAVES: But if I could just go down that track a little bit, when you talk about elite practice, one of the questions in my mind for which I do not have an answer is, who's going to agree to it? I mean, clearly, two people have to agree on something. One is the provider, but then the question for me is who's going to agree from the Assembly's perspective, having regard to separation of powers? For example, I would be aghast if I had to depend upon doing my job properly and appropriately if the Chief Minister of the day has an agreement with the provider. The relationship I might have with my constituent organisations and individuals has got absolutely nothing to do with what the government of the day has.

Mr Hart: I think you may regard this relationship as being with the clerk of the Assembly.

MR HARGREAVES: Well, that is an answer. Another answer might be that the arrangement is with the Speaker, because in fact the clerk is an officer of the parliament and the Speaker in fact is the elected head of that parliament.

Mr Vanderheide: It is probably not an answer that we can give you, Mr Hargreaves. It really is going to be up to you to determine.

MR HARGREAVES: I guess where I was coming to is: is there a precedent for that? Is always the relationship in the other jurisdictions with the clerk or equivalents or it is with the parliamentary officers?

Mr Hart: The responses we were provided with by those other jurisdictions didn't go into that degree of detail. I think a couple of them mentioned that they had agreements in place.

MS DUNDAS: And there is a Speaker's committee in New South Wales that, I think, monitors them.

Mr Hart: This is a new area. I think to some extent we are doing a bit of trail blazing with these protocols.

MS DUNDAS: There is discussion about separation of powers and setting up serviceable agreements with the Assembly, be that through the Speaker or the clerk, but you're still under the direction of the minister as part of the executive and you're still part of the government. That could leave you in a situation where you are—

MRS DUNNE: You're serving two masters in a sense.

MS DUNDAS: Yes. You're working for two masters in a sense, and that impacts on our role as an Assembly. So currently how is that being managed, and how do you think it should be managed into the future?

Mr Vanderheide: I guess I would say that in my experience—and that is not that long with InTACT but certainly is longer with ACT government—we haven't had that kind of conflict to resolve between our minister and another direction.

Mr Hart: Can I refer back to the email breach, because the potential situation actually occurred then. Although what happened then wasn't codified in a practice document, obviously we were collecting a large volume of information on who did what to whom and when, and that was on individuals in the Assembly. We had an obligation to keep our chief executive informed in general terms about what was going on. That was a brief acting at the direction of the clerk of the Assembly and so forth.

The department developed an internal understanding that no material left in InTACT could be identified or identified people. The general manager of the day was making those calls, about whether it was appropriate for a piece of information to be passed up the line. That was after some internal discussion within InTACT. The practice during a pretty tense time actually worked out for the government. That relevant information didn't leave the operational area. So, while that wasn't codified, that is how it worked. I think the sorts of issues that you're moving into now are really beyond us as a provider to give a definitive answer to but the practice last time wasn't a problem.

MRS DUNNE: So the message that I am getting, Mr Chairman, is that perhaps in a sense, the Assembly has to decide what level of security and what level of separation, and then InTACT can fall in with that decision.

Mr Hart: Absolutely.

MR SPEAKER: Under the service level agreements—if I can create another hypothetical for a moment—let's assume we've got a draft service level agreement, and we want not only to be separated but also to be seen to be separated in some formal way. You as an agency of the territory responds to one of the ministers, so it seems to me that the agreement we would have to reach would be with the relevant minister. Then in turn you would be bound by the service level agreement. Do you see it working that way?

Mr Vanderheide: I am seeing it could work that way. It hasn't in the past. To my knowledge, ministers have never been involved with the service level agreements we've established with agencies or with the Assembly.

MR SPEAKER: But we are a bit of a different animal.

Mr Vanderheide: Absolutely, yes you are. We can fit in with pretty much any model that you guys want to adopt.

MR SPEAKER: In the scheme of things, somebody's got to be held accountable for all of these issues if something goes wrong. The only person that we can hold accountable is the relevant minister, and so far as the Assembly is concerned the only person that it can hold accountable probably is me. Obviously, we will go through this with later witnesses but that is one possible direction.

MRS DUNNE: I suppose going on from that—this moves off security as such but on to day-to-day practicalities—in the Assembly we have a desktop which is essentially the bulk standard desktop, whether you're an ASO2 or the Chief Minister. I suppose it is an issue that arises with Val—why can't I do X? I can do it at home but I can't do it here.

There are a whole lot of protocols in InTACT that sort of limit the sorts of things you can do. For someone like a member who does a fair amount of monitoring of news and stuff like that, there is a whole lot of stuff that you actually can't access because you do not have the software on your machine to run the video or run the audio and things like that. It is the constant bane of my life. I could go out and buy the transcript but that costs a bomb, but if I could listen to the audio file, that is all I need and we just can't do that.

Mr Vanderheide: What I would encourage you to do—and you may have done this already—is speak to Val about what your needs are. Val will speak to us and we will do everything we can to make it possible—where we can make it possible. I think you're referring to audio streaming, which we do not generally allow because it means punching a hole in our external firewalls so the data can come in and this creates the potential for a security breach. There may be a way around it.

MRS DUNNE: That is just a for instance.

Mr Vanderheide: We will work to make possible whatever you need to have done. If you need something loaded onto your machine, the appropriate channel is through Val to us. We test it to make sure that it is not going to do anything to anything else on your machine, so sometimes some time is involved in actually making it work and there is some cost involved in getting the stuff to do that and put it on.

Mr Hart: There are a few issues. There is a cost issue. InTACT has to recover its costs, and if it is a software that requires a licence fee then that licence fee has to be recovered from the agency.

Mr Vanderheide: But it doesn't sound like you're concerned about that. You obviously are, but you're not raising a cost issue, you're raising a service issue.

MRS DUNNE: No. Another example, a lot of us have digital cameras. The one that I have won't run on the software because you can't run a USB board. So I spend a fortune sending pictures from home, ruining my download allowance at home, because I can't load them here, but they're work-related things.

Mr Hart: The common question that we are asked and that deserves an answer is: why can't I load this free piece of software on my machine? It's a reasonable question and the answer to it is that if we give you the opportunity to load this free piece of good software on your machine yourself, that opens a significant security weakness in that you can load bad pieces of software. The New South Wales parliament encountered exactly that problem where they didn't have their workstations locked down and a member of staff put all sorts of interesting network packet-sniffing tools and hacking tools on his machine because he could, and he was inside a place where it was in his interests to do that. So it is one of those eternal tensions between functionality and security, and that's a judgment call.

MRS DUNNE: Yes. So it might be that there needs to be a protocol that says, I would like to put X on my machine because it is convenient for me. Somebody has to say, yes, it is not going to cause a problem, or no, I really do not think we can do this, I am terribly sorry. And you have to live with that decision because there is a hierarchy of needs. You can't, by wanting to load something that is convenient onto a machine, completely wreck the system for the whole network.

Mr Vanderheide: Worst case, yes.

MRS DUNNE: It won't happen then, but it is the thin edge of the wedge, or are you opening a small portal that will create another problem. If we could come up with a protocol for dealing with those things, where somebody makes a judgment and you say, good, thank you, or next, that would be useful.

MR SPEAKER: I am sure that there is a kaleidoscope of free software and stuff out there that would end up in the hands of members one way or another. It would become a hell of a job to get it all on in a secure way.

Mr Vanderheide: It is also possible for us to establish a machine that is separate from the network that you can do what you want with basically. It is not going to have an impact on anything else that is running in here or elsewhere in government. That may be an option as well.

MR SPEAKER: All right. Are there any further questions? Are there any other issues that you'd like to raise with us?

Mr Vanderheide: No. I would reiterate that the options that we put forward were based around things that we know we can do. We will work to whatever solution you seek. We could, as I said, mix and match between what we've got and we can dream up other solutions. We will do that in conjunction or in close co-operation with whoever you elect as the appropriate body for us to deal with.

MR SPEAKER: All right. Thanks very much for putting the time aside and coming to see us. I trust that if we need to see you again you will make yourself available?

Mr Vanderheide: You know where we are.

MR SPEAKER: Thanks very much.

Sitting suspended from 10.28 to 10.44 am.

TOM DUNCAN,

RUSSELL LUTTON,

VAL SZYCHOWSKA and

IAN DUCKWORTH

were called.

MR SPEAKER: I should go through the formalities. You should understand that these hearings are legal proceedings of the Legislative Assembly protected by parliamentary privilege. That gives you certain protection but also certain responsibilities. It means that you are protected from certain legal actions such as being sued for defamation for what you say at this public hearing. It also means that you have a responsibility to tell the committee the truth. Giving false or misleading evidence will be treated by the Assembly as a serious matter.

Welcome to this inquiry. Would you like to make some opening comments?

Mr Duncan: Mr Speaker, I would. For the benefit of the record, I'm Tom Duncan, the acting clerk of the Legislative Assembly. I have with me Russell Lutton, who is the Manager of Hansard and Communications, on my right. Val Szychowska, the IT Manager, and Ian Duckworth, the Corporate Manager, are on my left.

Mr Speaker and members of the committee, we have made a submission to this inquiry that you'd be well aware of. The tone of the submission is that we put forward a model that basically entails going with the current IT provider, that is InTACT, but with some caveats and modifications. They are outlined in the submission. The only thing we would like to add is to comment on a couple of items that the previous witnesses gave evidence to. So at some stage, if we've got time from your questions, we might like to add to the comments that were made by the previous witnesses.

MR HARGREAVES: Mr Speaker, could I ask Mr Duncan et al to do that now?

Mr Duncan: Yes, sure.

MR HARGREAVES: That would be helpful if we had it up front.

Mr Duncan: Okay. Well I think one of the issues mentioned was the representation of the information management group, and either Russell or Ian would like to talk on that issue.

Mr Lutton: I will kick off with one of the key points—

MRS DUNNE: Now, Russell—

Mr Lutton: Sorry, Russell Lutton, Hansard and Communications.

MRS DUNNE: I enjoyed that.

Mr Lutton: I was breaking the first rule there. I think one of the key points that we've been trying to make in our submission—and it's obviously a key point in the committee's mind—is establishing with InTACT that appropriate level of separation and having from them a recognition that the Assembly is not part of the whole of government; it's separate from the executive government, separate from government agencies.

I think we've seen a fairly significant move on InTACT's part in relation to that. I come, I suppose, with the disadvantage and the advantage of being here for a relatively short time. But reading what's happened before and seeing the change in attitude that's come, particularly since some change in management in InTACT, it has been pretty refreshing. I think my colleagues would support me on that.

One of the things that would need to happen, though, as a result of that is a recognition of the Assembly's role in several of the major boards of management and bodies that are set up to oversee the way the IT service provision operates. In other words, we'd be looking for an equal place, an equal footing in those bodies. That's not always the case at the present time. Val represents us at a range of meetings and fora and does so very well. I think we would be looking for an elevated position in that respect.

MRS DUNNE: So more than one vote at the table, is that what you're saying?

Mr Lutton: No, a vote at the table rather than no vote at the table.

MS DUNDAS: Maybe to use an example, the previous witnesses mentioned an IT group that has heads of departments and it's chaired by Mr Tonkin from CMD. I would assume the Assembly is not in any way involved in that. So the whole-of-government decisions that are made at that meeting for InTACT and IT service providers just apply to us without any say in that forum? Is that an example of what you're talking about?

Mr Lutton: Yes, it is, a perfect example.

MR HARGREAVES: And a solution for that would be?

Mr Lutton: Having our representative on that board.

MR HARGREAVES: If it's a forum of chief executives, it would be appropriate for the clerk to be represented on it?

Mr Duncan: Can I just pass to Ian Duckworth, Corporate Manager?

Mr Duckworth: I guess I wouldn't mind just adding to that view and putting it in a little context. I understand the previous witnesses referred to three levels or three groups at work. Val participates and the Assembly has participated quite actively in the lowest level, the departmental information officer level. I don't think there are any particular issues there. For the next level up they've developed a concept of CIOs or chief information officers, and I think that was very much driven by the Department of Urban

Services who had massive IT issues. That tends to work at the more strategic level and I think that's a group where we would certainly value having a contribution.

With the next level up, the information management board, which involves chief executives of all agencies and chaired by Rod Tonkin, I could envisage issues being raised in that forum that are not necessarily relevant to the Assembly. Maybe a solution is that there be some recognition that the Assembly is a player in the scheme of things, that there is an organisation or group with an IT need, and that we have the opportunity to have input into that group without necessarily forming membership of that group.

I'm not at all certain what particular issues are raised and discussed but I could imagine that it could be involved in seeing cabinet submissions and clearing cabinet submissions on issues. That could make the Assembly's participation awkward, but I certainly think that being represented only at the lowest of the three rungs we're missing out on an opportunity of being represented at the second level.

MR HARGREAVES: Always one of the questions in the back of our minds is whether or not we want to be part of a larger organisation or a stand-alone unit. Having regard to the economies of scale, you naturally would go with the larger organisations, with costs and so on. But unless you're in at that top level, even though you're playing a very relatively small part in it, you're not going to be aware of any of the larger-scale changes which may impact on the decision about whether to go your own way or stay part of a wider issue. It's information power stuff. It just seems to me that the power of making that decision is not the main part of it.

Mr Duckworth: Just to clarify, I wasn't advocating not participating. I was just indicating that full participation could, from time to time, give rise to possible conflicts, particularly given the separation of powers issue that is the key issue to this inquiry.

MRS DUNNE: Mr Speaker, it seems to the completely uninitiated in matters of IT—I use it but I don't know how it works, sort of thing—that the separation of powers issue is actually important and Ian touches on some important issues there. We may be better served by a service level agreement of a fairly high order and maintain our separation through that, and perhaps not participate in the high level discussions about what departments want; that we do that through addressing our own needs through a service level agreement. I'm open to persuasion one way or the other, but I think that Ian raises important questions about conflicts of interest and the blurring of the separation of powers if we're involved at a higher level in the management of InTACT rather than perhaps being in a client relationship with InTACT—but perhaps a client with some clout.

MR SPEAKER: How do you respond to that?

Mr Duncan: I think Mrs Dunne's right. If the committee decides to go down the path of the Assembly staying with InTACT, the point we're trying to make is that we need to be informed, we need to keep abreast of what's happening with InTACT. If that's done at the highest level of the board, the chief executive level, I share the same sort of sentiments that Ian has, that there are issues there in relation to separation of powers.

If it were the position of the clerk to be on that board, I'd probably find it a bit incongruous in some respects. Some of the things don't relate at all to the secretariat role of the Assembly and have much more to do with government. It's probably inappropriate that the clerk should be there. Having said that, if we are part of that system, there are some whole-of-government issues that we need to be kept abreast of. We need to be kept informed so that we can provide the services to members.

MRS DUNNE: I suspect there are other mechanisms of keeping abreast of those issues though.

MR SPEAKER: Let's assume that the group, board, whatever they call themselves, make a decision about a certain matter. A service level agreement ought to leave it open to us to contest those ideas, if we felt it's an issue that concerns us, and bounce it back to the board, or group, whatever they call themselves.

Mr Lutton: I think it's a case of finding the right level of representation. But it also gives the Assembly a forum at which to ensure that its position in the system of government, and its needs, are very clearly represented.

I don't think that's always been the case in the past and it would be a very useful way of finding the right level of representation. "This is an issue for the Assembly, do you realise it's not part of the government departments?"—which I think until very recently hasn't been picked up by anyone.

MR HARGREAVES: Presumably each CEO has brought to the table a group of peculiarities of that particular agency. So the problems experienced by that agency and shared by others would be actually fixed in a corporate kind of way. In that sense we're talking about a mechanical service available to an agency; we're not talking about policy direction or the actual service delivery end in that department. We are just talking about the mechanical processes. Perhaps in that sense the Assembly is no different. If an agency brings a particular problem to the corporate table and finds resolution, and that resolution compromises a separation of powers, then we wouldn't be there at the time to say, "Hang on a second, have you thought of blah blah?" As I understand it, we're just talking about a mechanical service.

So, I have to differ a bit in the worry about being in there and being subject to a conflict of interest. If we were talking about CEOs coming together and talking about implementation of policy, you'd be spot on the money. But we're talking about provision of a service. One of the issues that the email problem raised was that we were regarded no more importantly than the file registry of the department somewhere, and that enabled that hiccup to occur. We were not right in their face with that separation issue, and if we don't do that we are going to be facing the same problem again later down the track.

Mr Duncan: Mr Speaker, I agree with everything everyone's said. The only problem is, having recently become acting clerk, I'm not exactly sure what the board does, and I'm not too sure whether my colleagues know. It may well be the committee wants to check with the Chief Minister's Department and seek some information about how it perceives the role of the board, what the board does, and what the other structures are in relation to IT in the ACT government, so the committee has a full appreciation of how that board operates and whether it would be appropriate for the Assembly to be represented.

MR SPEAKER: That's something we might consider a little later, yes. You may have heard some discussion about service level agreements with InTACT. Who do you think we should be reaching the agreement with, if we were to have one?

Mr Lutton: InTACT.

MR SPEAKER: But InTACT is then under the general umbrella of the executive. We've got to try to hold somebody accountable here if something goes wrong with the system. Would it be appropriate for us to sign a service level agreement with InTACT, and then have it endorsed by the executive or some process like that? Does that present problems?

Mr Duncan: I'll let Russell lead and I might add something.

Mr Lutton: Mr Speaker, I honestly don't know, having come to work in this environment fairly recently. But I was discussing this broad issue with Michael Vanderheide at morning tea. It could well create some tensions for InTACT. We are treating InTACT as our IT service provider. We would want to enter into an SLA with them that reflected our unique needs in relation to the sorts of issues Ms Dundas and Mrs Dunne raise. So, it would really be an issue for InTACT to be able to go to Treasury and say, "We're providing these services in this context. We're answerable to the Assembly for this, not to Treasury."

MR SPEAKER: But you'd have to get executive agreement to that.

Mr Duncan: Yes. We were talking about this when the issue was raised by InTACT as to who the service level agreement would be between. I suspect that you might have to have two service level agreements. One between the clerk of the Assembly and InTACT, and another higher policy type agreement between the Speaker and the relevant minister in charge of InTACT to talk about the big picture type issues.

MRS DUNNE: If we were going out to ABC Wizard as an IT provider, that's how it would work. The clerk would have a contract with the private provider and there would be another arrangement to ensure that Treasury funded that. I suspect that Russell is correct, that the day-to-day interaction is with InTACT, and that Tom's suggestion that you need two agreements might be the way we have to go. I'm just trying to visualise. If InTACT were a private entity rather than a government entity, that's how it would work.

Mr Duckworth: I was just going to add some comments to what Mrs Dunne just said. InTACT was born in '96, and the Assembly formed its first relationship with InTACT in January of '97. We've never had a service level agreement with InTACT. We've had two drafts that got very, very close to being final before—for various reasons I won't go into—they blew away, or dismantled, or extinguished, or evaporated. We've never had a signed service level agreement.

I don't think it matters who provides our IT service. There would have to be an agreement with whoever is the provider. As Mrs Dunne just indicated, if that was a private company, we would have some sort of an agreement. The agreement in its simplest form is: "You give us services, we give you money." We should have that sort of agreement with InTACT, and could have with InTACT, in the sense that if they don't deliver we can adjust the billing—we don't pay their charge or we have that sort of remedy available to us.

Where I think we've got a particular issue, and what I think Mr Speaker may have been referring to, is that InTACT as an entity reports to the executive. If this inquiry is about dealing with the separation of powers, how do you have separation if the executive ultimately controls InTACT as an agency? Potentially we do have a bit of a conflict in that model because IT can sometimes get a bit sensitive if there is a particular issue. I would be concerned if a non-executive member reported to us that they didn't think one of their staff was doing quite the right thing. There might even be some elements of criminal activity or whatever. If we report that to the AFP, and there's a protocol in place between the AFP and the police minister, there's an obligation in that model, in that system, for the executive to be informed about what's going on in the parliament. I think there's a tension there, potentially. I'm not suggesting people wouldn't do their best to treat the information properly. That is a potential problem with this model.

At the end of the day, if the concern of the committee is that the executive shouldn't be in control of parliament's information, then there should be some higher than a service level agreement—some sort of a memorandum of understanding between perhaps the Speaker and the Chief Minister, or the Speaker and the executive as a whole—about how these sorts of situations should be escalated and managed. It would be particularly important if, heaven forbid, anything did go wrong, that the Assembly has the right to manage its information and its issues independently without that level of—I don't like to use the term interference because I don't think it would be that level of involvement.

MRS DUNNE: But even knowledge sometimes is.

Mr Duckworth: I'm not proposing a solution. I am just simply identifying and I think there's an inherent conflict in them all.

MR HARGREAVES: At the risk of sounding pedantic about it, one of the things that occurs to me about the service level agreement is that it's assuming that the parliament is the same as an agency within the public service—Urban Services, Chief Minister's, education, whatever you like. It assumes that we are an agency, because service level agreements are swapped between agencies to give service, and such is not the case. Whilst I don't want to appear pedantic, if we agree that parliament is quite a separate being altogether, and has different relationships entirely, then nothing needs to be exchanged between the ministers per se—the Speaker being a minister from parliament—and somebody else; rather a full-on contract. Parliament chooses whether to go to selective tendering. So, if you have a full-on commercial arrangement with the government provider of the IT service and if there is a breach of that contract, then parliament decides to drop the contract and go with another provider. It would then go to outside, if necessary.

The risk is, again, without seeming pedantic, perhaps it is the relationship, the preservation of the separation part of that relationship, which can have its voice by using a full-on contract instead of a service level agreement. It struck me then that service level agreements are all about swapping stuff between agencies. The minute we do that we are no different, we are just parliament, just part of the bureaucracy for the purposes of this exercise.

MS DUNDAS: On that point, can I ask a quick question? Tom, in your opinion as acting clerk, could the Assembly sue the government for breach of contract?

Mr Duncan: Obviously we would have to take legal advice on that. If we've signed a contract, I would imagine that, like any agency, we've got the right to take remedies for it. Whether we can sue someone would depend—

MS DUNDAS: But Mr Hargreaves was just proposing an actual contract and separating ourselves as a normal agency. If worse come to worse, you're suing for breach of contract.

Mr Duncan: I would assume that the contract would have remedies for breaches or failure to deliver services or failure for us to pay or things like that. Hopefully, if the contract is properly made up, it would cover the eventualities that Mr Hargreaves has outlined.

MR SPEAKER: Service level agreements are a contract by another name.

MR HARGREAVES: They are, except that they actually perpetuate the relationship between an interagency approach. It is one of the difficulties, in fact, that community service organisations have had in their relationship with the government in the grant process. They come up with a service level agreement because they're getting grants. But they're not actually contracted to provide a service. So therein lies a tension. When they don't perform, the government just chops off their grant. But there's no sort of comeback. It's a very poor relationship between the community organisation and the government of the day.

MR SPEAKER: But at the end of the day, if a service level agreement is not satisfactory and is not being satisfactorily responded to, it would always be open to us to say to them, we've finished with you lot, we're going somewhere else. The same would apply if there was an arrangement between the Assembly and a minister—the same thing.

MS DUNDAS: In your submissions you have a summary of your preferred model—a greater level of organisation and unit separation. You refer to some basic parameters you'd like to see—the Assembly taking over and running the administration and first and second-level user support. To help us get a clearer picture of this model can you explain how you would see that operating and how it would be different to what we have now?

Mr Lutton: Ms Dundas, we haven't actually fleshed out exactly how we would see that operating, but we'd certainly like to see a much tighter level of control within the Assembly of things like account management and perhaps issues like Mrs Dunne referred to—the particular pieces of software. If it is possible to facilitate this, then we should be doing it. Obviously all agencies, all departments, need to have locked-down environments. This place isn't unique in that respect.

But we would like to have someone who works with us, who knows the InTACT tentacles and how things work. We would like to have, as I say, a much-improved control over things like account management, which includes email accounts, obviously, and I think we'd sort of have to feel our way. It could even be done on a rotational basis so that the people who support us work with us for a period and develop that knowledge of the Assembly and its different place—we're not a run-of-the-mill department.

MS DUNDAS: That is similar to, say, a departmental liaison officer working in a minister's office?

Mr Lutton: Not dissimilar, that's right.

MS DUNDAS: But the person providing user support, a technical officer, we already have Val, who's working in liaison and on-site management. Is what you mean bringing in another technical officer to work with Val to fix the minor day-to-day problems like spilling coffee on our computers or whatever, that kind of stuff?

Mr Lutton: Or mice that break.

MS DUNDAS: Yes. So the team that we have working in the building is what we're getting at. We currently have two—Russell, as manager of the whole unit, and then Val, in her role. So we're actually bringing in a third person to do technical support and the account manager. So that would be one person doing both of those things. They would establish accounts, clear up any problems in file management et cetera. Then the support that would be coming from InTACT would be the network support, the WAN support, that kind of stuff?

Mr Lutton: Yes.

MS DUNDAS: That is what you're envisaging?

Mr Lutton: That's right. As I say, to be quite honest, we haven't really defined our need there and we started to think about it and we thought that in the available time we'll make our claim for this. An issue of real concern for us is account management, and a lot of things flow from that.

There is that level of first-line support. I have to take a very high-level view of this, given the amount of Hansard work I'm involved in. Val, too, does a lot of work with InTACT and whole-of-government forums and project-related work. I think it would be very useful for us to have someone—and if we continue with InTACT, it would have to be someone from InTACT, because they know both sides. We want to develop that relationship better. It could well evolve over time, Ms Dundas.

MR SPEAKER: Have you seen the options put forward by InTACT?

Mr Lutton: Originally I'd seen them in their paper. We had not seen their submission until last Friday.

MS DUNDAS: I guess the options they put forward are the same ones that we saw?

Mr Lutton: Yes, they are.

MS DUNDAS: Many, many months ago.

Mr Lutton: And not dissimilar from the Acumen ones, except they moved things one step further with the introduction of that common operating environment 2000.

MR SPEAKER: Does one of those options match your preferred model or go close to it?

Mr Lutton: Yes. We're saying the same thing, Mr Speaker.

MR SPEAKER: Which one?

Mr Lutton: We're saying that we should set up a separate organisational unit.

MR SPEAKER: Which option was that?

MS DUNDAS: I think it's option No 2 or option No 3.

Mr Lutton: Yes. If you're looking at their original paper, Mr Speaker, and not their submission, which was May 2003—

MR SPEAKER: I'm only looking at their submission, which may not be very helpful.

Mr Lutton: They've embedded it in a lot of other issues. But basically they're proposing to set up the Assembly's IT structure as a single organisational unit.

MS DUNDAS: I think it's option 3.

Mr Lutton: Option 1 for them was to maintain the current arrangements without change. Neither the Assembly nor InTACT is saying that's acceptable. They're proposing option 3, establishing a separate organisational unit. They recognise that setting up the Assembly and separating it with a firewall is an option. They're recognising that applying that model with two firewalls is also an option. If you read the Acumen report that the secretariat had done to assist the committee, both those options don't appear to provide any increased level of security—if that is a major concern of the committee.

There are still exposures in those sorts of models and they come at considerable cost. I don't believe we're saying that at a point in time the Assembly may not want to go on a different route, which could encompass one of those; we're saying at the moment that the model they're proposing, establishing the Assembly as a separate organisational unit, as a more or less sealed entity within the whole-of-government IT infrastructure, is probably the appropriate way to go.

MR SPEAKER: That's option 3.

Mr Lutton: That's correct.

MRS DUNNE: That would mean that we're no longer linked to the Chief Minister's server or any of those things?

Mr Lutton: No, it doesn't mean that.

MRS DUNNE: It doesn't?

Mr Lutton: No. One of the projects that we are currently involved in is partitioning the disk on which the executive, non-executive, and secretariat data is stored. Currently it's held on one server. We are now involved in a project to partition that information so that if someone with mal-intent wanted to try to access information from those three discrete sections of government, they can't do so. That is a mandatory first step to establishing the separate organisational unit. While we haven't today done an SLA, we haven't introduced Assembly-specific security arrangements. Doing that was something we felt we could constructively do that pending some guidance and direction from the committee on this.

MS DUNDAS: On the diagram that you provide at the back of your submission you separate the non-executive, the executive, and the staff. Would that mean two little extra computer mainframes on the diagram to get the physical representation of that?

Mr Lutton: Yes.

MS DUNDAS: So they would sit under the organisational unit? There'd be the LA non-executive, the LA secretariat, and the LA executive?

Mr Lutton: How would that work, Val?

Ms Szychowska: At the moment InTACT has a partition that encompasses the data for the secretariat, the non-executive, and the executive. There are pros and cons for the management and support of that arrangement. We want to separate that so they're implementing security policy to restrict access to each of those areas. While we have a separation of data, where that data sits on the network is not the issue. It's just that it's stored on the whole-of-government server farm and it rents space on the ACT government network on a server amongst other agencies. The policy they will put in place on our data will ensure that where administrators will get access to, say, the executive arm of the data they will not have access to the non-executive arm of the data.

MS DUNDAS: We wouldn't need separate service level agreements for secretariat, non-executive, and executive? It would be all covered by the one?

Ms Szychowska: Yes.

MRS DUNNE: There seems to be a level of agreement that best, most desirable model is a separate stand-alone entity for the Assembly in dealing with InTACT, so that we're not seen as part of government. That wouldn't necessarily translate into the sort of physical infrastructure? You might have a sort of separate organisational structure, but when it comes to where the data is stored on what server, that wouldn't necessarily translate. So you wouldn't end up with a Legislative Assembly server, is that right?

Ms Szychowska: That's right.

Mr Lutton: That's right. That's not what is proposed at this stage.

MRS DUNNE: Okay. Is it not desirable to have a separate server, or doesn't it matter? Is it the protocols that underpin the structure of the server that's the issue rather than the actual physical separateness?

Mr Lutton: I'd take guidance from Val and Ian on this because at one stage in the past the Assembly did have a separate server and we were convinced that it was in our interest to locate our data on a shared server at another location. But my understanding—at a high level I acknowledge, Mrs Dunne—of what's being put to us is that it doesn't matter. What matters is how our information is partitioned and separated.

Ms Szychowska: Any IT service provider will tell you, with the solution that is proposed in this scenario, it doesn't matter if it's a physical separation or a logical separation, one or the other will have less or more work involved in maintaining it. Prior to the 2000 upgrade we had an environment where we weren't able to divide our data and provide local security arrangements. Now it is possible with the new 2000 environment. We can now put in what they call logical security policies that basically provide the same result as if you had a physical security. To provide and support a physically separate environment would take a lot more resources, cost and effort to implement and maintain. The suggestion that InTACT provide in their submission, the option of providing an organisational or domain, which is like a logical separation, would achieve the same thing and require less resources and cost.

MR SPEAKER: But there was an issue about whether we ought to have an organisational separation and a domain of our own too. The domain in turn requires more effort, and InTACT seems not to be that confident that they have the immediate expertise to deal with a domain. How do you respond to that?

Ms Szychowska: I sought clarification on that issue. Apparently InTACT indicated that the domain model was to implement a solution prior to the 2000 upgrade. That's the advice I was given. The domain structure and the organisational unit are essentially the same thing. One's a little bit more logically separated than the other, but in terms of security it's really up to the skill of the service provider to put in the expertise to secure it.

MR SPEAKER: Which is the most secure? It is suggested that it is the domain.

Ms Szychowska: Yes. More secure, but that's a theoretical thing. It really depends on the expertise of the service provider. Organisational will achieve almost the same level.

MR SPEAKER: At significantly less trouble?

Ms Szychowska: Yes.

Mr Lutton: Mr Speaker, could I just pick up on a point that Mr Hargreaves was making re contracts and SLAs. Clearly the committee will make its decision on this but I don't think we would expect any SLA we entered into with InTACT, if that were to happen, would represent the run-of-the-mill type of SLA that InTACT enters into with government agencies. If we were to continue with InTACT we would have a very different document here. Whether it's in the SLA or in attached associated protocols, we would need to address the type of issue that Ms Dundas raises and a range of other issues that are Assembly-specific ones.

MR SPEAKER: You seem to place emphasis on the accounting arrangements, and I think it was having separate accounting arrangements?

Ms Szychowska: Administration.

MR SPEAKER: Administration and accounting.

Mr Duckworth: Mr Speaker, you may be looking at the term "account management".

MR SPEAKER: Account management, okay.

Mr Duckworth: An account in this context is effectively a new staff member starting and being granted access to the network and being given an email address. That's called setting up an account. It's interesting because I was just about to add some comments to what Russell was saying about the service level agreement being tailored. Having had the IT responsibility transferred to Russell's area a year ago, the corporate officers are still grappling with the cost and the bills. I would think that whatever direction the issue goes, one issue that must be addressed with InTACT is their billing, their accounts, the actual charging—as distinct from the accounts we were just talking about.

MRS DUNNE: Physical money.

Mr Duckworth: It is a nightmare, an absolute nightmare. We've made no secret of that to InTACT. I don't think that will come as any great surprise. I'm certain that Michael Vanderheide gets the same feedback from other agencies. If we ended up going down our own path and eventually developing a service level agreement with InTACT, I think we would seek to call the shots on how accounts should be submitted at the moment. We are very much driven by the whole-of-government approach to billing.

MR SPEAKER: But Mr Lutton seemed to have an emphasis on the account management issue, aside from the billing arrangement. I'd like to hear a little bit more on that.

Mr Lutton: Obviously there are several scenarios. A new staff member starts in the building and needs access to the Microsoft suite of products. They might need specific business applications, they need email. Currently, that's handled through the help desk. It's not just new starters. One of the big issues is staff moving between offices.

MR HARGREAVES: Or stopping altogether.

Mr Lutton: Yes, that's right, Mr Hargreaves. That needs to be very carefully tracked and managed, as InTACT have learnt. You know they have condensed the number of staff doing this. But we are proposing that that should be more firmly controlled by the Assembly itself. If we were to continue with InTACT, probably the best person to have would be somebody from InTACT. When a new person starts in the building clearly support can be provided, given the nature of members' work, in setting up the applications, in providing assistance to new staff, to members, about how things should operate. It's not appropriate that someone in a member's staff or a member is just told, "Here's your account, here's what you've got." I think assistance needs to be provided.

What we're saying is—and we're not sure of the appropriate watermark for this—that there should be someone assisting us in doing this.

MR SPEAKER: So it becomes driven in-house but supported by InTACT?

Mr Lutton: Yes.

MR SPEAKER: I understand, yes.

MRS DUNNE: So you wouldn't necessarily have recourse to the InTACT help desk but rather an in-house InTACT person here?

Mr Lutton: Yes.

MR SPEAKER: So, if I've got a problem or I've just arrived or I'm just leaving or going somewhere else, I ring you and then you organise everything else to happen.

Mr Lutton: It's a fair point. We would have to work out very carefully what protocols apply. Obviously, Corporate is notified when a new contract is raised. We would have to be notified. There would have to be just plain procedures developed so these things are tracked internally. They do apply now. We have to say that InTACT appears to be doing this very well but there will be times—

MR HARGREAVES: But InTACT wouldn't have a clue whether a person is put on as a volunteer. If they're given access to the system and they stop being a volunteer, the members themselves don't know when the person's going to stop being a volunteer.

MRS DUNNE: He says, "Whatever happened to—".

MR HARGREAVES: Yes, exactly, "didn't notice he wasn't here".

MR SPEAKER: So, this service level agreement will have to have some in-built flexibility so that it can grow to suit the exigencies of the Assembly?

Mr Lutton: Yes. There are several associated issues. The Assembly should have its own security policy. It's been put on hold for some time; it's not there. The Assembly should have a common user policy that applies to all of us.

That's not going to be the whole-of-government policy. That was the issue of that splash screen that came up and told you "thou shalt not do this or that". That has to be developed, it has to be accepted, it has to be there—that everybody recognises I'm using this system under certain rules, which obviously don't include passing on your password to somebody else. So it's accepted that this is the type of environment in the security and operating sense we're working within.

MS DUNDAS: I'm picking up on that small point there. In the ream of paper that you've provided on current working arrangements, you noted that you applied the policies developed by the ACT information group where practicable, and attached to that were the last witnesses. How is that monitored and maintained when they've set up a policy that's meant to apply to the entire whole-of-government network to maintain security and a bunch of us are sitting here doing something completely different because we're not necessarily aware of it or it doesn't apply? How is that managed from your end? In setting up our own policies, how would you see that relationship working?

Mr Lutton: I'll go once again at a high level and obviously Ian and Val would have some good background information to apply. We more or less apply that de facto. I think InTACT, given what happened with the email affair, has been very happy to step back and not try to force on the Assembly any whole-of-government security policy.

MRS DUNNE: But the default is that we have no security policy.

Mr Lutton: That's right, in a nut shell. If we were to develop one, the approach I would take is we'd look at their generic one, we'd look at the one at Parliament House, we'd look at the one at New South Wales parliament and come up with a model to apply to bring to the committee for consideration. It may not be too different from the InTACT one but it could be quite different in some key respects.

Mr Duckworth: I would just add to that that I think it's probably true that we don't have a clearly articulated document called a security policy. I would probably beg to differ that we don't have a security policy blank, because I think we do. I think we have certainly sets of arrangements that, if you like, our practice complies with. We don't actively encourage people to share passwords. We do have identified people who are able to authorise. What I'm saying is there's not a complete vacuum. There are policies and procedures and practices in place that respect the need and identify the need for certain security, but it's certainly true that we need to tailor something to this organisation. I think Russell's point was that that's probably a project or an issue that has in some respect been put on hold in awaiting the outcome of this particular inquiry.

Mr Lutton: That's certainly true, Mrs Dunne. My response to you was at a higher level—can I give you a document that says this is the Assembly security policy.

MS DUNDAS: So, the example of the email warning system that we were talking about that attaches to emails that leave the building—the disclaimer—that was a whole-of-government policy that came in from InTACT and we adapted it to suit Assembly purposes because of differences there?

Ms Szychowska: It came through the ISG, the whole-of-government meeting that I attend. They raised the issue that they want to implement it at a whole-of-government level. I brought it back through management. It was raised with Mr Speaker in your committee and we went through the process of deliberating whether it suited our purposes. Now, the dependency from the ACT government point of view was that if the Legislative Assembly staff members decided that it didn't suit and they didn't want to implement it, it wouldn't be able to be implemented across the board without significant technical overhead. So, it was either all in or none at all. We deliberated and decided that, with some minor changes, it would be put in place so it will go in with the whole of government.

MS DUNDAS: So messages coming from the Assembly have a different disclaimer on them to the rest of the whole of government, or have our amendments to that disclaimer been taken up by the rest of government?

Ms Szychowska: Yes, they have been.

MS DUNDAS: And that was the only way it could have been done, every one that left the network had to have the same disclaimer?

Ms Szychowska: That particular issue and solution, that's right.

MS DUNDAS: Even if we go down the path of the administration separation, would there be scope to have that completely distinct disclaimer or no disclaimer at all, as a hypothetical example, whilst still being part of the InTACT system?

Ms Szychowska: Yes.

MS DUNDAS: It could have happened in the past, it was just chosen not to?

Ms Szychowska: Yes. In IT circles, everything is possible. It's just a case of dollars.

MS DUNDAS: Sure.

Mr Duckworth: To add to Val's comments, Ms Dundas, I think this is another example of where a very relevant and focused service level agreement—if that is the course that's followed—should identify that level of detail. It would seem to me that virus management is going to be something that's going to continue to occupy many, many minds for many, many years to come. If the ultimate model is a more separate Assembly environment, but against an InTACT backbone, if you like, we'd want to take advantage of their virus management capability rather than try to replicate that ourselves. So there'd be issues of their entire network management that we'd want to tap into and we'd want to apply to us We'd want also to be able to say, look, if a Chief Minister, a chief executive or the information management board decreed that this is going to happen, we need to have the ability to opt out of that. That needs to be recognised by both us and InTACT, so that we can manage that process.

Some earlier examples were the splash screen, if you like, that people saw—that some in this place argued was very much a government theme, and therefore they didn't like that.

MRS DUNNE: I must have missed that. It must have been one of those long periods where I didn't log off.

Mr Duckworth: I think we're all saying we need to have that independence, ability to manage.

MR SPEAKER: Are there any further questions?

MR HARGREAVES: No.

MR SPEAKER: That being the case, I'd like to thank you all for putting the time aside. If we need to call you again, you'll hear from us.

The committee adjourned at 11.40 am.