The Legislative Assembly for the Australian Capital Territory

Inquiry into InTACT Service Provision in the ACT Legislative Assembly

Report No. 4

Standing Committee on Administration and Procedure

November 2003

Committee membership

Mr Wayne Berry MLA (The Speaker of the ACT Legislative Assembly)

Ms Roslyn Dundas MLA

Mrs Vicki Dunne MLA

Mr John Hargreaves MLA

Secretary: Mr Tom Duncan

Inquiry Secretary: Mr David Skinner

Administration: Ms Judy Moutia

Resolution of appointment

1. Inquire into and report on, as appropriate:

    a. the Assembly's annual estimates of expenditure;
    b. the practices and procedure of the Assembly; and
    c. the standing orders of the Assembly;

2. Advise the Speaker on:

    a. Members' entitlements including facilities and services;
    b. the operation of the transcription service (Hansard);
    c. the availability to the public of Assembly documents;
    d. the operation of the Assembly library; and

3. Arrange the order of private Members' business and Assembly business.

Terms of reference

1. Inquire and report on…:
    (1) the role of InTACT as the Legislative Assembly IT service provider.

Table of contents

Summary of recommendations

RECOMMENDATION 1

The committee recommends that the Assembly and the Government, where relevant, agree to the implementation of the IT service delivery model as identified in paragraph 2.33 of this report including:

a) the establishment of the Legislative Assembly as a separate 'organisational unit' in the larger ACT Government network;

b) the provision of the necessary human and financial resources to undertake the separation and consequent implementation of the model on a recurrent basis;

c) that the Assembly Secretariat assume responsibility for account creation and management (both email accounts and user login accounts);

d) migration of the Assembly's email system to a software solution that allows the Assembly to assume control over email account creation and management at the earliest possible opportunity; and

e) the engagement of a dedicated technical officer (preferably sourced from InTACT) reporting directly to the Assembly IT Manager, and responsible for responding to staff requests and onsite troubleshooting.

RECOMMENDATION 2

The committee recommends that a memorandum of understanding be developed between the ACT Executive, through the relevant Minister (at the present time, the Treasurer), and the Legislative Assembly, through the Speaker, which clearly affirms that:

a) there is distinct separation of the roles and functions of the executive and legislative arms in the ACT's system of Government, requiring that the Assembly have managerial and institutional autonomy with regard to the operation of its IT network and data storage;

b) in terms of InTACT's development, servicing and maintenance of the Legislative Assembly's IT network and data storage, InTACT reports not to the ACT Executive but to the Speaker via the Clerk of the Assembly;

c) the ACT Executive undertake not to interfere in the administration and operation of the Assembly's IT network and data storage; and

d) information stored on and communicated via the Assembly's network will not be passed on to personnel operating under the direction of the ACT Executive (ie InTACT and departmental officials) without the specific agreement of the Clerk and having regard to matters of parliamentary privilege.

RECOMMENDATION 3

The committee recommends that the Assembly Secretariat develop and implement a service level agreement or contract for service between InTACT and the Assembly that:

a) includes timeliness standards (including response and resolution timeliness standards);

b) includes billing policies and procedures;

c) includes quality standards;

d) includes remedies for poor service against standards;

e) requires that all InTACT staff involved in servicing the Assembly's IT needs be made aware of, and understand, the memorandum of understanding between the Speaker and the Minister responsible for InTACT;

f) affirms that the Legislative Assembly, through the Assembly IT Manager, is responsible for account creation and management on the Assembly IT network (both email and user login accounts);

g) affirms that the dedicated InTACT officer (seconded) reports to the Assembly IT Manager and not InTACT;

h) acknowledges the need for the Assembly to have the capacity for Members, their staff and Secretariat staff to achieve a degree of customisation on their desktop computers such as the use of software for digital cameras (where such customisation does not present security or copyright issues);

i) stipulates that the integrity of the Assembly's data is protected to a high degree (in the event of a systems failure) through adequate backup and storage provisions; and

j) stipulates the Assembly policy on the creation and management of email and user login accounts.

RECOMMENDATION 4

The committee recommends that, as a matter of urgency:

a) the Assembly Secretariat develop and implement an IT security policy and associated procedures for all staff, outlining responsibilities and the broader IT security arrangements and procedures (including procedures setting out the circumstances under which email and user login accounts can be created, removed and managed as well as how regular maintenance should be undertaken by technicians, having regard to the need to gain consent from the relevant Member or their delegate to create, remove or perform maintenance on an account); and

b) the Assembly Secretariat develop and implement an education and awareness program on the IT security policy as well as on general IT security issues, for delivery to all non-Executive Members, their staff and Secretariat staff.

RECOMMENDATION 5

The committee recommends that Government make provisions for the Assembly to be given increased opportunities for consultation and providing input on whole-of-government IT issues, by way of involvement on the Chief Information Officer forum, where those issues potentially have an impact on service delivery for the Assembly.

Chapter 1. Introduction

Background

1.1. This inquiry arose directly out of a recommendation of the 2002 report of an Assembly Select Committee on Privileges that inquired into the unauthorised diversion and receipt of a Member's emails.[1]

1.2. That committee was established by the Assembly to investigate, 'whether the unauthorised receipt of emails from Mr Wood's office was a breach of privilege and whether a contempt was committed'[2].

1.3. As part of that committee's investigations, the role of InTACT, the Assembly's IT (Information Technology) service provider, was called into question. Indeed, the Privileges Committee made some trenchant criticisms regarding the performance of InTACT and expressed the view that the Standing Committee on Administration and Procedure should review InTACT's role in servicing the IT needs of the Assembly.

1.4. In its submission to this inquiry, InTACT itself acknowledged its failings, concurring with the Privileges Committee's assessment that the incident in question, 'reflects very badly on InTACT'.[3] That committee went on to conclude that, 'At almost every step their [InTACT's] processes seem to have failed either because staff ignored them or their procedures were inadequate'.[4]

1.5. This committee acknowledges that a serious breach of security occurred in relation to the diversion of email incident and this report is directed towards ensuring that the Assembly, as an institution, is properly protected from a similar incident occurring again.

1.6. The committee has also considered a range of broader issues associated with the Assembly's management of its computer network.

Scope of the report

1.7. The reference adopted by the Assembly for this inquiry simply tasked the committee with inquiring into and reporting on, 'the role of InTACT as the Legislative Assembly IT service provider'. The committee refined this general reference and made the decision to examine and report on:

- **Governance issues** – the articulation of a set of principles for the development of robust governance structures which clearly delineate the separation of the

[1] Known hereafter as the Privileges Committee
[2] ACT Legislative Assembly, Minutes of Proceedings No. 22, 6 June 2002 para 20.
[3] Select Committee on Privileges (2002) '*Unauthorised diversion and receipt of a Member's emails'* Legislative Assembly for the Australian Capital Territory, p 20.
[4] Ibid, p 20.

legislature from the executive with respect to the management of the Assembly's electronic communications and data storage on its IT network as well as the need for service standards and improved contract management provisions to effectively manage the Assembly's business relationship with an IT provider.

- **The adequacy of current IT security provisions** - what steps has InTACT taken to ensure that an incident of the type investigated by the Privileges Committee is prevented from happening again, as well as any other security measures that have been implemented?

- **A preferred service delivery model** – what is the most appropriate model for the Assembly's IT service provision in relation to the different approaches proposed by witnesses and submitters?

Conduct of the inquiry

1.8. At the commencement of the inquiry, the committee advertised in the local press as well as writing to other parliaments to seek information about the range of approaches for managing IT services in legislatures around Australia.

1.9. The committee subsequently received four submissions (listed in Appendix A).

1.10. The committee also sought a submission from the ACT Government seeking its views on the performance of InTACT, but, as of the time of writing, the committee had not received one.[5]

1.11. On 5 May 2003, the committee received a private briefing from the IT and Security Manager for the Tasmanian Parliament.

1.12. On 10 September 2003, the committee conducted a public hearing, taking evidence from InTACT and the ACT Legislative Assembly Secretariat.

1.13. During the course of the inquiry and pursuant to Standing Order 239, the committee also called for papers from both the Legislative Assembly Secretariat and the Chief Minister's Department; pertaining, respectively, to the Secretariat's business relationship with InTACT and the role and functions of the whole-of-government Information Management Board chaired by the Chief Executive of the Chief Minister's Department.

Summary of Conclusions

1.14. After considering the matter, the committee decided that it is appropriate for the Assembly to continue using InTACT as its IT provider but that the establishment and implementation of effective governance structures, policies and contract management procedures must be afforded the highest priority.

---

[5] The committee did receive a submission from InTACT.

1.15. The committee reviewed the findings of the Select Committee on Privileges report on the diversion of a Member's emails, particularly in relation to InTACT's failure to provide adequate security measures for the Assembly's IT network, but concluded that since the incident, InTACT has significantly improved its security provisions. While the committee believes that InTACT's performance in relation to the diversion of a Member's email was extremely deficient, it concluded that a new security-minded culture is being introduced in the organisation and that the degree of technical expertise in this area has been considerably enhanced.

1.16. However, as a separate issue, the committee came to the view that decisions about how the Assembly will manage its relationship with InTACT must be underpinned by the rigorous application of the separation of powers doctrine. That doctrine holds that the three arms of government: the legislature; judiciary; and the executive, must be independent from each other and that the powers exercised by each do not come into conflict.

1.17. Due to the fact that InTACT operates under the direction of the executive arm of government through its reporting chain to the Treasurer, the committee is concerned that under current arrangements there is a potential for InTACT's role in servicing the Assembly's IT network (a primary means of communication for non-executive members) to come into direct conflict with its role in reporting to the relevant Minister.

1.18. For instance, as one example, it is conceivable that sensitive information derived from a non-executive Member's computer by an InTACT technician could be passed up the reporting chain to a current or future government minister. To prevent any such conflict, the committee believes that more stringent governance arrangements must be put in place and to this end, the committee has recommended that steps be taken to formalise the relationship between InTACT, through the relevant Minister, and the Assembly, through the Speaker.

1.19. The committee wishes to put firmly on the record that the Legislative Assembly is not, in any conception, analogous to a government department in that it has no reporting or accountability responsibility in relation to the ACT Executive. The executive arm, should not oversee or impeach the operations of the Assembly, including interference in the management of the ACT Legislature's IT systems.

1.20. The committee was presented with several different service delivery models for consideration and has recommended that while InTACT should continue to provide IT services for the Assembly, it is necessary to explicitly codify the nature of that relationship.

1.21. The committee concluded that:

- the Assembly should continue to use InTACT as its service provider (albeit under an enhanced governance and contract management

framework);

- the fact that the Assembly is quarantined from executive interference vis-à-vis the management of its IT systems must be clearly articulated and encoded in a memorandum of understanding between the Legislative Assembly and the ACT Executive;

- improved security provisions must be introduced to logically separate the Assembly IT network from that of the ACT Executive (including the separation of non-Executive, Secretariat and Executive data);

- the Assembly be given increased control, administrative access, and autonomy in the management of its IT network to the extent that Assembly decisions do not affect the security and functionality of the larger ACT Government network managed by InTACT – particularly in responding to the individual, often idiosyncratic, IT needs of members and their staff; (there is a need, in some cases, to go beyond the locked-down whole-of-government standard operating environment - for instance the use of proprietary software for digital cameras);

- as a key client of InTACT, the Assembly must have the capacity to provide input into whole-of-government decisions regarding IT issues which affect it – this should involve increased/improved representation of the Assembly in whole-of-government IT fora;

- increased resources need to be allocated to the Assembly to provide for more effective management and maintenance of its IT network and associated infrastructure (primarily through the creation of a dedicated Assembly IT Network Administrator position);

- improved contract management provisions should be introduced, in the form of a service level agreement (SLA) or contract, to ensure a high degree of InTACT responsiveness to the Assembly's IT needs;

- an Assembly IT Security policy needs to be developed; and that

- an education and information program needs to be developed and implemented to provide advice to Members, their staff and Secretariat staff as to their responsibilities regarding IT security and to raise awareness about IT security matters generally.

1.22. The committee addresses these issues in more detail in the following chapter of the report.

Chapter 2. Issues

2.1. This chapter of the report outlines the main issues considered by the committee as well as conclusions and recommendations to arise from its investigations.

Diversion of email

2.2. Without recapitulating all the events that transpired in relation to the diversion of a Member's email, the committee thought it worth briefly summarising the main issues to arise out of the privileges report, specifically related to InTACT's role in the incident.

2.3. The incident investigated by the Privileges Committee related to the diversion of a series of emails intended for Mr Bill Wood MLA (a then newly appointed Minister in the ACT Government) to the computer of a volunteer working out of the office of the then Leader of the Opposition, Mr Gary Humphries MLA.

2.4. According to the Privileges Committee, the breach appears to have been the result of InTACT re-establishing a lapsed account of Mr Wood MLA, bill.wood@act.gov.au, and improperly diverting mail received at this address to the Opposition volunteer in question. The Privileges Committee noted that:

> Prior to the election Mr Wood had only used the 'WOOD' [WOOD@act.gov.au] mailbox. The 'bill.wood' address had been cancelled at a much earlier time. Mr Wood and his senior adviser Ms Watt were unaware of the existence of the new 'bill.wood' mailbox, had not requested it and did not use it. For technical reasons this mailbox was not displayed in Mr Wood's Microsoft Outlook home page.[6]

2.5. In its report, the Privileges Committee concluded that, 'The process of diversion was not accidental. It could not, plausibly, have happened as a result of a random conjunction of keystrokes. Nor is there any evidence of hacking into the InTACT system from outside having occurred'.[7] An investigation undertaken by the Australian Federal Police (AFP) concluded that:

- the modification of MS Exchange Server settings requires system administration rights, and access to the appropriate software tools; and
- accordingly the person responsible for this diversion being created is almost certainly an InTACT employee…[8]

---

[6] Selection Committee on Privileges, '*Unauthorised diversion and receipt of a Member's emails*' November 2002 ACT Legislative Assembly. p 9.
[7] ibid p 10.
[8] Detective Senior Constable Frank Gill to Mr Ken Archer, Office of the Director of Public Prosecutions, 8 May 2002, p2 cited in ibid.

2.6. It is of considerable concern to this committee that InTACT's own internal governance and risk management arrangements were unable to prevent the unauthorised diversion from occurring and more concerning still is the fact that the likely source of the diversion was from within InTACT itself.

2.7. Equally disturbing is the fact that InTACT's network logging/accounting system proved inadequate in terms of ascertaining exactly who committed the breach and when. As the Privileges Committee noted, 'The police also found that because of the way InTACT backups are kept it was not possible to identify either the source of the diversion or the date it occurred with any more accuracy [although police identified the likely date of the diversion was 27 November 2001]'.[9]

2.8. It is important to point out that, in the course of the Privileges inquiry, InTACT claimed that there were no well-established procedures in place between the Assembly and InTACT stipulating under what circumstances, and with what permissions, InTACT staff could instigate an email diversion of the type that occurred. The Privileges Committee found that:

> InTACT advised the committee that the second mailbox was created in accordance with what they believed to be the normal practice of the Assembly to provide members two email addresses. Because they were re-establishing, rather than creating a system it does not appear that InTACT were acting on any specific instructions from Mr Wood's office. Nor did InTACT seek any specific authority from Mr Wood or his office to provide the second mailbox.[10]

2.9. The committee believes that the lack of a specific Assembly IT security policy on how accounts are to be created, disbanded and maintained must be addressed and the committee speaks to this later in the report.

2.10. In response to members' questions on the diversion of a member's emails, InTACT was candid with the committee making clear that it accepted responsibility for the lapse in security. InTACT told the committee that:

> …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.[11]

2.11. InTACT advised the committee that one of the problems that lead to the breach of security was that its security focus had been, up until the time of the incident in question,

---

[9] Selection Committee on Privileges, '*Unauthorised diversion and receipt of a Member's emails*' November 2002 ACT Legislative Assembly. p 10.
[10] ibid, p 9.
[11] Transcript of proceedings, 10 September 2003, p 2, Mr Vanderheide.

primarily directed towards external threats to the ACT Government network rather than potential security risks that existed internally. InTACT noted in evidence that, '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'.[12] In this regard, it appears that not even a rudimentary risk management strategy was in place to deal with the potential security risks associated with the inappropriate diversion and redirection of emails from within InTACT itself.

Changes to security arrangements

2.12. InTACT informed the committee that it had implemented several measures to improve the level of security offered by the organisation to ensure that incidents similar to the matter investigated by the Privileges Committee are prevented from happening again. In its submission, InTACT advised the committee that security enhancements have been pursued in three main areas: technical improvements, administrative and policy improvements, and improvements to staffing arrangements within the organisation. The details of work undertaken by InTACT on these three fronts are outlined below.

Technical security enhancements

2.13. InTACT has undertaken technical improvements in several areas including:

- dramatically reducing the number of staff with system administration privileges;
- active monitoring of changes to administrative privileges – which independent audit has stated to be the most effective system of its type in the ACT; and
- major improvements to logging and monitoring.[13]

2.14. InTACT explained to the committee that where there used to be over 80 staff with the requisite level of administrative access to divert/redirect email, there are now just over 20 staff with this level of access privilege who are all required to undergo a security vetting process.[14] This committee is supportive of these measures and notes InTACT's comments in the public hearing that it is, 'recognised as running something that is pretty close to best practice across government in terms of the security vetting process'.[15]

2.15. The committee was also pleased to learn that InTACT has introduced better monitoring and logging systems for tracking unusual actions on the network and to ensure that administrative actions on the network can be traced should a similar incident occur again. InTACT advised the committee that:

---

[12] ibid, p 2, Mr Vanderheide.
[13] Submission 2, p 4.
[14] Transcript of proceedings, 10 September 2003, p 3, Mr Vanderheide.
[15] ibid, p 3.

> 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.[16]

2.16. The committee is pleased to learn that these provisions are now in place both as a means of ascertaining which staff are performing what actions on the Assembly network as well as providing the clear disincentive for its staff to perform an action of the type investigated by the Privileges Committee.

Policy and administrative enhancements

2.17. InTACT has introduced the following policy and administrative improvements:

- InTACT now has a security internal audit program in place. Audits consist of a mix of compliance audits (how well are existing policies and processes being followed) and management audits (how can the current policies and processes be improved);

- a security education and awareness program, both within InTACT and across government; and

- InTACT has a robust vetting policy in place, with supporting processes. The Public Service Commissioner has expressed the view that InTACT now leads the rest of the ACT Government in this regard.[17]

2.18. Again, the committee is supportive of these new measures. The capacity for InTACT to review its compliance against the new policy provisions endows the organisation with the ability to ascertain any weaknesses and put in place steps to improve security in an ongoing manner.

2.19. The committee also believes that the increased emphasis on education and awareness regarding security matters is an important development. Indeed, the committee believes that a similar program must be introduced in the Assembly and speaks to this later in the report.

---

[16] Transcript of proceedings, 10 September 2003, p 4, Mr Vanderheide
[17] Submission 2, pp 4-5.

Changes to staffing arrangements

2.20. In its submission to the inquiry, InTACT advised the committee that at the time of the email security breach, there was only one InTACT officer responsible for network security matters – an officer positioned in a line area which was two reporting levels away from the General Manager. InTACT informed the committee that the following changes have been implemented to enhance security provisions in relation to staffing:

- the security monitoring, policy and investigation group has been split from the operational area, and now reports directly to the General Manager;
- the staffing levels in security have been increased by four since the breach;
- the security group is now headed by a career information security professional; and
- the overall expertise of the security function is now much higher, and includes, for example, former Defence Signal Directorate staff.[18]

2.21. The committee is pleased that the degree of security-specific expertise has been increased in InTACT and believes that the tighter reporting arrangements (directly to the General Manager) represent a major improvement.

2.22.The committee is satisfied that all the new security and risk management arrangements put in place by InTACT provide a significantly enhanced security regime but as with all areas of risk management, InTACT must be ever-vigilant in ensuring that security threats (external and internal) are reviewed on an ongoing basis and that prevention and mitigation strategies are continuously monitored, revised and improved.

2.23. However, despite the introduction of all these changes, the committee understands that during the course of the inquiry an incident occurred whereby InTACT inadvertently deleted an email account of the Leader of the Opposition, Mr Brendan Smyth MLA. The committee understands that this occurred as a result of an InTACT effort to delete a large number of generic 'public accounts' and that SMYTH@act.gov.au was included on the list of accounts to be deleted. While the committee accepts that the oversight was an honest mistake, without malicious intent, it is nonetheless an unacceptable mistake which adversely affected Mr Smyth's office's electronic communications for a period of time.

2.24. Later in the report, the committee advocates that the Assembly assume control for account creation and management and that a dedicated technical officer position be established. The committee believes that the incident described above highlights the importance of the Assembly assuming greater control over account management and makes a recommendation to this effect.

[18] Submission 4, p 5.

Service delivery models

2.25. In early 2002, following a resolution of the Standing Committee on Administration and Procedure, the Assembly Secretariat engaged a consultant (Acumen Alliance) to undertake a review with the purpose of providing expert advice on the various service delivery options available to the Assembly in relation to the provision of its IT services. In May 2002, Acumen Alliance presented the Secretariat with its report, *IT Service Delivery Options, Evaluation Report*, which presented three different options for the committee's then consideration. They were:

1. continue outsourcing with InTACT (the current arrangements);

2. appoint a non-government outsourced IT provider; and

3. reduce outsourcing and increase the Assembly's involvement in IT service provision.[19]

2.26. In their submissions, both InTACT and the Legislative Assembly Secretariat make reference to different service delivery models for the committee's consideration. While InTACT makes no recommendations in its submission as to a preferred model, the Secretariat includes in its submission, an evaluation of each of Acumen's proposed approaches, outlining the costs and benefits associated with each, culminating in the articulation of a Secretariat position on the matter which is distinct from the options proposed by Acumen.

2.27. The first option proposed by Acumen Alliance was that the status quo be maintained and that the Assembly continue utilising InTACT for IT service delivery under existing arrangements. The Assembly Secretariat, in its submission, expressed concerns that this was an unsuitable approach, as it does not adequately address issues associated with the imperative to ensure the effective separation of powers. The Secretariat expressed the view that this option was inadequate noting that:

> [The Secretariat's objections are] based on the fundamental tenet of our system of government: the legislature, the executive and the judiciary are independent and separate arms of governance. The offices and systems that support them should likewise be independent and separate. The Assembly should control the security and privacy of its electronic data.
>
> As the report of the Select Committee on Privileges on the unauthorised diversion and receipt of a member's emails (November 2002) demonstrates, the current model does not provide a satisfactory level of separation from government or the necessary level of security and privacy for the Assembly's electronic data.

[19] Submission 4, p 2.

> In this context, the report of the Select Committee on Privileges on the unauthorised diversion and receipt of a member's emails (November 2002) raises questions about whether the current model provides a satisfactory level of separation from government and the necessary level of security and privacy for the Assembly's electronic information.[20]

2.28. As noted, the committee also has significant concerns about continuing with the current approach and particularly the lack of arrangements that clearly affirm the autonomy and independence of the Legislative Assembly to manage its IT services. Later in this report, the committee proposes a governance framework to overcome the current difficulties.

2.29. The second option conceived of 'using a private IT service provider (ie, not InTACT) and separating the Assembly's IT environment from the executive and the ACTGOV whole-of-government environment'.[21] It was envisaged that physical separation would be achieved by introducing a firewall to physically separate the Assembly network from the ACT Government network. The Secretariat also expressed concerns about the suitability of this model noting that:

> The Acumen report identified several risks and shortcomings associated with this option… The Secretariat believes that there are other potential risks and disadvantages associated with option 2. For example, the record of government agencies obtaining satisfactory service from outsourced private IT providers is poor. Potentially, this model would require much higher levels of management and coordination than the current model. The interaction between the outsourced private IT provider and InTACT, with the Assembly in the middle, potentially adds a new layer of complexity to day-to-day IT management.
>
> Based on Acumen's indicative costings…, this model would yield significant savings to the Assembly after the initial establishment costs had been met. However, there are hidden costs that are difficult to quantify; and it introduces risks and disadvantages that would have to be very carefully managed. Most importantly, Acumen notes that the risk of a breach of data security is the same as for the other options…
>
> There may come a time when, based on a confluence of circumstances—the size of the Assembly, cost/standard of services received from InTACT, changes in technology or a break down of the existing ACTGOV whole-of-government network—this is a feasible option. It is not the Secretariat's preferred model at this time.[22]

2.30. The third option proposed that the Assembly IT environment be separated from the ACT Government network through a firewall whereby InTACT would continue to

---

[20] Submission 4, p 2.
[21] Ibid, p 2.
[22] Ibid, p 2.

provide all services outside the firewall[23] while the Assembly would control all services on its side of the firewall.[24] The Secretariat made the following comments regarding this approach:

> While there are substantial establishment costs associated with this option (Acumen's estimate, $143,000 v InTACT's estimate, $170,000 to $190,000), Acumen acknowledges that the security risk "remains the same as with the current situation". An InTACT senior network administrator, or the administrator of the private company under option 2, would have access to the firewall to effectively manage it.
>
> At the time the Acumen report was prepared—before the migration to the Windows 2000 operating platform—this option probably best met the Assembly's requirements of creating a separate computing environment and providing a higher level of security and privacy for its data, while maintaining links with the whole-of-government network and commonality of operating platform.
>
> The introduction of the Microsoft Windows 2000 operating system offers another option to separate the Assembly's electronic data and to restrict access to nominated users.[25]

Secretariat's preferred model

2.31. Finally, in its submission, the Assembly Secretariat proposed an alternative service delivery model based on the following key requirements:

- It must provide a high level of service to the Legislative Assembly.
- It must provide a clear separation for the Legislative Assembly IT systems from those of the other arms of government.
- It must offer a high level of security and privacy for electronic data.
- It must retain the current level of data backup and connectivity with the InTACT whole-of-government IT infrastructure.
- The implementation and ongoing support costs must be commensurate with the results sought and achieved.[26]

2.32. The committee is supportive of these guiding principles.

---

[23] Firewalls are a means of managing the access between computer networks. There are both logical (software based) and physical (hardware separation) firewalls.
[24] Submission 4, p 3.
[25] Ibid, p 3.
[26] Ibid, p 3.

2.33. Based on these requirements, the Assembly Secretariat proposed a preferred model and the committee considers that it is worth reproducing the Secretariat's stated preference in its entirety.

> In mid-2002, InTACT, in close consultation with the Legislative Assembly IT Manager, investigated and reported on network "separation" options offered by Windows 2000. One option available under what Microsoft calls the Windows 2000 "active directory" service is the establishment of separate "organisational units"[27] within a network. Information on the active directory service and organisational units is at attachment 1.
>
> Using the Windows 2000 software it is possible to establish a separate organisational unit—eg, the Legislative Assembly—within a network, such as the whole-of-government network, and to implement tight controls over who has access rights to data within the organisational unit—eg, only registered users in the Legislative Assembly organisational unit.
>
> The advice from InTACT's security managers is that if the appropriate technical architecture and administrative protocols are implemented in association with creating the Legislative Assembly as a separate organisational unit, a high level of separation and security can be achieved for the Assembly's data.
>
> Importantly, this model allows for local control over account management, including the allocation and withdrawal of access rights to individual users, although InTACT can continue to do this if required. The Secretariat believes that control of account management should be the responsibility of the Assembly[28].
>
> It would still be necessary to provide external access to Assembly data to a limited number of InTACT central server facilities (CSF) staff and support staff. InTACT is prepared to have the access and security processes it applies to the Legislative Assembly organisational unit regularly audited. CSF staff have Highly Protected level security clearance.
>
> The Secretariat-preferred position would be for this access to be further limited by having an InTACT technical officer dedicated to work on site at the direction of the Assembly IT manager. This would be an additional cost but it would provide a much higher level of support and separation for the Assembly's computing systems. This person would be responsible for first and second level support such as responding to staff requests for assistance and on-site troubleshooting.

---

[27] The committee has included an explanation of the terms 'organisational unit' and 'active directory' as they relate to IT networks, as Attachment 1.

[28] The committee notes that there are two types of account management regarding the Assembly's IT network. There are email accounts and user login accounts. The model proposed by the Secretariat envisages that the Assembly would be responsible for managing both.

Third level support issues generally require technical expertise, and these would be referred back to InTACT because it has established change control processes to address these.

In presenting this model to the committee for consideration, the Secretariat is conscious of the advantages derived from the links the Assembly has to the ACTGOV network. These include:

- Operating on common standards and an integrated computing platform with ACT departments and agencies —eg, operating system, redundancy and data back up, virus control, network management.

- The use of common email address lists and the Internet, which makes electronic business transactions with ACT government agencies quick and convenient.

- InTACT has positioned the Assembly well with its IT strategic planning.

- InTACT's capacity to undertake IT-related projects in an IT environment that it operates and has detailed knowledge of.

The Secretariat considers that this model meets the criteria set out above. It is also flexible in that its establishment costs are low and it does not preclude the Assembly's adopting a different model in the future if this were identified as being necessary.

InTACT estimate the establishment cost at about $10,000. This does not include Assembly staff time or the cost of developing a service level agreement (SLA), which the Secretariat regards as essential. A major component of the SLA would be a clear recognition by InTACT of its responsibility to the Assembly, not to its minister or to executive government, for the delivery of Assembly IT services [the committee speaks to the issue of an SLA in the following section of the chapter].

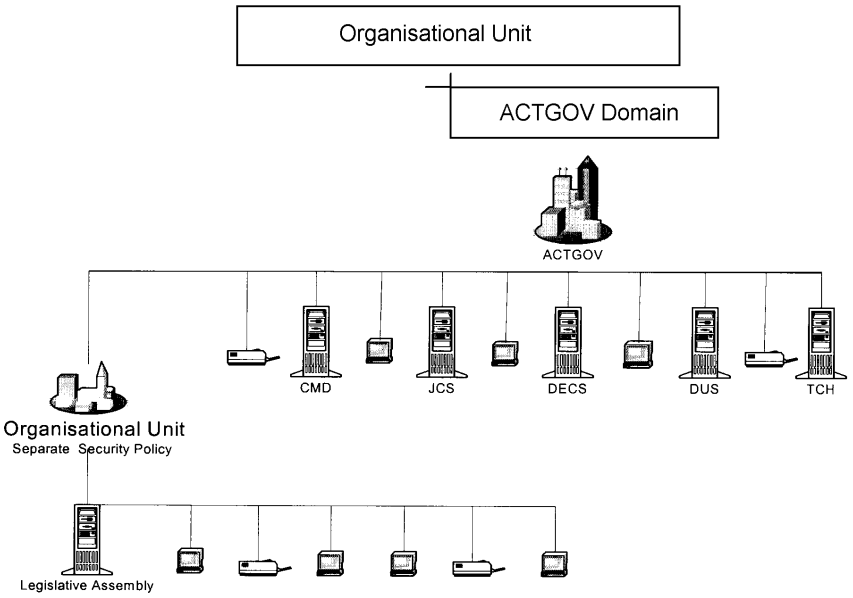
The duration of the project is estimated at eight weeks. The timing of the project and involvement of Assembly staff would have to be considered in the context of other workload. It may be necessary to take a staff member off line and/or engage a contractor.

The Assembly IT manager is currently undertaking a project with InTACT to segment disk space available to executive members, non-executive members and Secretariat staff (project PO1217). This places the Assembly in a good position if the organisational unit model were accepted. The data division that will result from project PO1217 represents a mandatory first stage of establishing the Assembly as an organisational unit.

Migration of the Assembly's email system to Exchange 2003 email would be necessary if the Assembly were to assume responsibility for account management. InTACT plans to move the Assembly to Exchange 2003 in December 2003. It has indicated that it is prepared to look at modifying the

project plan to bring the Legislative Assembly migration forward if this were required.[29]

2.34. The following diagram illustrates how the technical separation of the Assembly's network would operate.



2.35. The committee is supportive of the model proposed by the Secretariat, believing that it:

- provides adequate separation between the ACT Assembly and the ACT Executive;
- fulfils security requirements for the protection of electronic data;
- is cost-effective; and
- provides increased organisational autonomy in the management of the Assembly IT system, particularly in relation to account creation and management (for both user login and email accounts).

2.33. The committee would like to see that the proposed model be implemented as a matter of urgency.

Recommendation 1

[29] ibid, p 3-5.

The committee recommends that the Assembly and the Government, where relevant, agree to the implementation of the IT service delivery model as identified in paragraph 2.33 of this report including:

a) **the establishment of the Legislative Assembly as a separate 'organisational unit' in the larger ACT Government network;**

b) **the provision of the necessary human and financial resources to undertake the separation and consequent implementation of the model on a recurrent basis;**

c) **that the Assembly Secretariat assume responsibility for account creation and management (both email accounts and user login accounts);**

d) **migration of the Assembly's email system to a software solution that allows the Assembly to assume control over email account creation and management at the earliest possible opportunity; and**

e) **the engagement of a dedicated technical officer (preferably sourced from InTACT) reporting directly to the Assembly IT Manager, and responsible for responding to staff requests and onsite troubleshooting.**

Data partitioning

2.36. The committee was informed that the Assembly Secretariat, in conjunction with InTACT, is currently in the process of segmenting or partitioning the data stored on the Assembly's network into three distinct areas with security access restrictions for each. The Assembly IT Manager informed the committee that:

> 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.[30]

[30] Transcript of proceedings, 10 September 2003, p 31, Ms Szychowska.

2.37. The committee is supportive of this work and looks forward to its completion. The committee understands that the Secretariat and InTACT are currently in the testing phase of the project.

Desktop customisation

2.38. During the course of the inquiry the committee raised the issue of the restrictions placed on Members and their staff in relation to their capacity to utilise particular software applications due to the locked-down standard operating environment. In response to a question from one of the members of the committee about the use of software that facilitates the capture of images from a digital camera via a USB (Universal Serial Bus) port, InTACT had this to say:

> 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.[31]

2.39. The committee is not satisfied with this response as the installation of the types of hacking tools mentioned by the witness are in no way analogous to the installation of proprietary software for use with a digital camera for example. Certainly there is a tension between functionality and security but, to date, it seems that InTACT has made these judgements without outlining substantive rationales for resolving the tension. In response to requests for additional software to be installed, too often it seems there is a default response to refuse the request on security grounds without necessarily evaluating, or at least communicating, the specific risks associated with particular pieces of software.

2.40. The committee believes that the Assembly needs greater latitude to install software beyond that which is provided as part of the standard operating environment. In this regard, the example of installing proprietary software for the use of digital cameras is a good one. Digital cameras can play an important part in the conduct of a Member's communication with their electorate enabling the production of newsletters and other materials on the activities that a Member undertakes in the community.

2.41. While the committee is not advocating that individual users be given access privileges to install software, it is appropriate for the Assembly to have the capacity and technical expertise (via the dedicated InTACT technician, the Assembly IT Manager and

[31] Transcript of proceedings, 10 September 2003, p 15, Mr Hart.

advice from InTACT) to evaluate security versus functionality issues on a case-by-case basis.

2.42. The committee addresses this issue in the recommendation it makes later in the report regarding the development of a service level agreement.

Governance issues

2.43. As stated in the first chapter of the report, the committee believes that more rigorous measures must be introduced to ensure there is fidelity in the relationship between InTACT and the Assembly vis-à-vis the separation of powers doctrine. To this end, the committee concluded that a memorandum of understanding should be developed between the Speaker of the Legislative Assembly and InTACT's relevant minister, the Treasurer, setting out the exact nature of the dividing line that must exist between the executive and the legislature in the oversight and operation of the Assembly's IT network.

2.44. There is also a need to better codify the Assembly's business arrangements with the provider to set out the levels of service expected; guaranteeing value-for-money, high-level security protection and exemplary customer satisfaction. The committee concluded that the best way forward on this front is to develop and implement a service level agreement (SLA) or contract which specifies the terms and conditions of the Assembly's business relationship with InTACT.

2.45. In evidence, the then Acting Clerk of the Assembly conceived a similar approach to addressing these two issues noting that:

> I suspect that you might have to have two… 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.[32]

2.46. The committee addresses these two separate issues below.

Separation of Powers

2.47. Without going into the theoretical minutia of the separation of powers doctrine, the committee thought is worthwhile briefly summarising the chief tenets of the doctrine.

2.48. The separation of powers doctrine was initially conceived by political theorists such as Montesquieu and Locke as a means of preventing despotism or absolutism in a system of government. The theory holds that there are three separate arms of government, all exercising different but discrete powers. As Graham Spindler notes in his paper, *'The Separation of Powers: Doctrine and Practice'*:

---

[32] Transcript of proceedings, 10 September 2003, p 25, Mr Duncan.

> The doctrine of the separation of powers divides the institutions of government into three branches: legislative, executive and judicial: the legislature makes the laws; the executive put the laws into operation; and the judiciary interprets the laws. The powers and functions of each are separate and carried out by separate personnel. No single agency is able to exercise complete authority, each being interdependent on the other. Power thus divided should prevent absolutism (as in monarchies or dictatorships where all branches are concentrated in a single authority) or corruption arising from the opportunities that unchecked power offers. The doctrine can be extended to enable the three branches to act as checks and balances on each other. Each branch's independence helps keep the others from exceeding their power, thus ensuring the rule of law and protecting individual rights.[33]

2.49. However, under the Westminster form of government, the legislative and executive functions/powers are not completely partitioned as the executive is formed from the membership of the legislature. As Spindler notes:

> Obviously under the Westminster System – the parliamentary system of government Australia adopted and adapted from England – this separation does not fully exist. Certainly in Australia the three branches exist: legislature in the form of parliaments; executive in the form of the ministers and the government departments and agencies they are responsible for; and the judiciary or the judges and courts. However, since the ministry (executive) is drawn from and responsible to the parliament (legislature) there is a great deal of interconnection in both personnel and actions. The separation of the judiciary is more distinct.[34]

2.50. While the *ACT Self Government Act 1988* does not explicitly set out the separation of powers, it is accepted that the ACT system of government is derived from a Westminster tradition and that its conventions, including the separation of powers doctrine, apply.

2.51. In the context of this inquiry the matter of the separation of powers becomes important due to the fact that the Assembly, as the legislature of the ACT, depends on an executive agency to deliver its primary electronic means of communication (via IT and phone networks), a crucial and fundamental function in the modern day parliamentary and political system. The integrity of these systems (IT systems being the focus of this inquiry) is paramount in ensuring that information produced by Members, their staff and Secretariat staff, and transmitted and stored on the Assembly's network, is quarantined from executive interference.

---

[33] Spindler, Graham '*The Separation of Powers: Doctrine and Practice'* in *Legal Date*, March 2000 accessed from http://www.parliament.nsw.gov.au/prod/web/phwebcontent.nsf/0/31aeed1097592aa0ca25693000316ab1?OpenDocument on 7 October 2003.

[34] Ibid.

2.52. While the committee accepts that InTACT is ultimately accountable to the ACT Executive in relation to its services, policy and financial management, it is not and should not be accountable to the executive in relation to the specific services it provides to the Assembly.

Memorandum of understanding

2.53. As noted above, the committee is of the view that it is imperative for the Assembly to better codify the separation of powers between the ACT Executive and the Legislative Assembly with regard to the management of the Assembly IT system.

2.54. The committee concluded that the best way to meet this requirement was to develop a memorandum of understanding (MOU) between the ACT Executive through the responsible minister, the Treasurer, and the Assembly, through the Speaker.

2.55. The committee makes a recommendation below as to the principles and affirmations that should be included in an MOU. This is not an exhaustive list of requirements and the committee is supportive of additional elements being included in the MOU that affirm the operational and institutional separation between the ACT Executive and the Assembly.

Recommendation 2

The committee recommends that a memorandum of understanding be developed between the ACT Executive, through the relevant Minister (at the present time, the Treasurer), and the Legislative Assembly, through the Speaker, which clearly affirms that:

a) there is distinct separation of the roles and functions of the executive and legislative arms in the ACT's system of Government, requiring that the Assembly have managerial and institutional autonomy with regard to the operation of its IT network and data storage;

b) in terms of InTACT's development, servicing and maintenance of the Legislative Assembly's IT network and data storage, InTACT reports not to the ACT Executive but to the Speaker via the Clerk of the Assembly;

c) the ACT Executive undertake not to interfere in the administration and operation of the Assembly's IT network and data storage; and

d) information stored on and communicated via the Assembly's network will not be passed on to personnel operating under the direction of the ACT

Executive (ie InTACT and departmental officials) without the specific agreement of the Clerk and having regard to matters of parliamentary privilege.

Contract management

2.56. It is of concern to the committee that there are currently no contractual arrangements in place between the Legislative Assembly and the IT provider, InTACT. The Assembly Secretariat advised the committee that it had come close to implementing a service level agreement with InTACT but for one reason or another it was never finalised.[35]

2.57. The committee came to the position that contractual arrangements in the form of a contract for service or service level agreement setting out the Assembly's requirements, service standards, and other basic business related stipulations, is required as a matter of urgency.

2.58. The committee has not been overly prescriptive in setting out the form that a contract or SLA should take but has instead recommended below the principles and key provisions that should be covered in any such agreement. Again, this recommendation is not intended as an exhaustive list of the provisions that might apply.

Recommendation 3

The committee recommends that the Assembly Secretariat develop and implement a service level agreement or contract for service between InTACT and the Assembly that:

a) **includes timeliness standards (including response and resolution timeliness standards);**

b) **includes billing policies and procedures;**

c) **includes quality standards;**

d) **includes remedies for poor service against standards;**

[35] Transcript of proceedings, 10 September 2003, p 21, Mr Duckworth.

e) requires that all InTACT staff involved in servicing the Assembly's IT needs be made aware of, and understand, the memorandum of understanding between the Speaker and the Minister responsible for InTACT;

f) affirms that the Legislative Assembly, through the Assembly IT Manager, is responsible for account creation and management on the Assembly IT network (both email and user login accounts);

g) affirms that the dedicated InTACT officer (seconded) reports to the Assembly IT Manager and not InTACT;

h) acknowledges the need for the Assembly to have the capacity for Members, their staff and Secretariat staff to achieve a degree of customisation on their desktop computers such as the use of software for digital cameras (where such customisation does not present security or copyright issues);

i) stipulates that the integrity of the Assembly's data is protected to a high degree (in the event of a systems failure) through adequate backup and storage provisions; and

j) stipulates the Assembly policy on the creation and management of email and user login accounts.

Security policy

2.59. One particular issue that was raised by the Privileges Committee was that there appeared to be no Assembly policy or procedure in place setting out how email account creation and management should be undertaken on Members and their staff's computers. The committee came to the view that the Assembly Secretariat should develop an IT security policy setting out the responsibilities of all Members, their staff and Secretariat staff as well as outlining broader IT security arrangements and procedures. The committee makes a recommendation to this effect below.

Education and awareness program

2.60. In its submission to the inquiry, the NSW Legislative Council asserted the importance of 'educating Members and their staff about the significance of computer security and the protection of passwords and files'.[36]

[36] Submission 1, p 1.

2.61. InTACT also advised the committee that it had undertaken an education campaign to improve the level of awareness on IT security issues across the ACT Government.

2.62. The committee agrees that the development and implementation of an education and awareness campaign on IT security issues for delivery to Members, their staff, and Secretariat staff, should be undertaken and recommends that this happen below.

Recommendation 4

The committee recommends that, as a matter of urgency:

a) **the Assembly Secretariat develop and implement an IT security policy and associated procedures for all staff, outlining responsibilities and the broader IT security arrangements and procedures (including procedures setting out the circumstances under which email and user login accounts can be created, removed and managed as well as how regular maintenance should be undertaken by technicians, having regard to the need to gain consent from the relevant Member or their delegate to create, remove or perform maintenance on an account); and**

b) **the Assembly Secretariat develop and implement an education and awareness program on the IT security policy as well as on general IT security issues, for delivery to all non-Executive Members, their staff and Secretariat staff.**

Consultation with Assembly

2.63. In evidence, InTACT advised the committee that currently there is a three level reporting structure on ACT IT matters. InTACT informed the committee that:

> There's a… Departmental Information Officer group, the… [Chief Information Officer] 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's chaired by Rob Tonkin (Chief Executive, Chief Minister's Department] and is comprised of all of the chief executives across government. On a monthly basis we provide a security update as to progress on projects that we've got underway associated with security so the level of interest in this is obviously very high as well.[37]

2.64. The committee learned that the Assembly only participates at the lowest level of the reporting and consultation structure, that is, at the Departmental Information Officer

[37] Transcript of proceedings, 10 September 2003, p 3, Mr Vanderheide.

level. In evidence, the Secretariat advocated that it would be useful for the Assembly to have increased involvement beyond this. The Secretariat advised the committee that:

> I understand the previous witnesses referred to three levels or three groups at work [regarding whole-of-government IT]. …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.[38]

2.65. The committee believes that it is appropriate for the Assembly to have input at the Chief Information Officer level, on issues that potentially affect it. It would be appropriate for the Manager of Hansard and Communications or the Assembly IT Manager to undertake a representational role in this forum.

Recommendation 5

The committee recommends that Government make provisions for the Assembly to be given increased opportunities for consultation and providing input on whole-of-government IT issues, by way of involvement on the Chief Information Officer forum, where those issues potentially have an impact on service delivery for the Assembly.

Telephones

2.66. The committee's broad reference for this inquiry primarily related to the role of InTACT in servicing the Assembly's IT needs, particularly in relation to the security and privacy issues arising out of the Privileges Committee report.

2.67. However, the committee was concerned that security provisions for the Assembly's fixed line and mobile telephone communications must be similarly protected. To investigate this matter further, the committee wishes to receive a briefing from InTACT as to what security provisions exist in relation to Members' and their staff's work telephones.

2.68. The committee will be writing to the Treasurer to seek this briefing in the near future.

[38] Transcript of proceedings, 10 September 2003, p 18, Mr Duckworth.

Conclusion

2.69. The committee was pleased that InTACT acknowledged its past failings in protecting the privacy and security of electronic communication on the Assembly's IT network and that it has taken step to rectify the problem.

2.70. Having reviewed the evidence presented by submitters and witnesses during the course of the inquiry, the committee is satisfied that InTACT has undertaken significant improvements in protecting the Assembly from security breaches of the type investigated by the Privileges Committee. The committee concluded that InTACT has adopted a new security-minded culture and that the level of technical expertise on security matters has also been enhanced substantially.

2.71. The committee is satisfied that the adoption of the recommendations in this report will produce an even greater level of security for the Assembly's electronic communications and data storage, above what InTACT has already achieved.

2.72. While InTACT will remain the Assembly's IT provider, the committee believes that the Assembly can do more to effectively manage its business relationship with the provider by way of improved contract management provisions. The committee also concluded that the Assembly Secretariat must develop an IT security policy and associated education and awareness program to meet its own corporate governance obligations.

2.73. The development and implementation of a memorandum of understanding between the ACT Legislative Assembly and the ACT Executive will also provide a more formal articulation of the fact that the Assembly is a unique InTACT client that requires a distinct organisational separation in terms of oversight and accountability.

Wayne Berry
Speaker of the ACT Legislative Assembly

November 2003

Appendix A – List of Submissions

1. The New South Wales Legislative Council
2. InTACT, ACT Treasury
3. Parliament of Australian, House of Representatives
4. The ACT Legislative Assembly Secretariat

Appendix B – List of Witnesses

Public hearing, Committee Room 1, Wednesday 10 September 2003

1. Mr Michael Vanderheide, General Manager, InTACT
2. Ernest Hocking, a/Director Service Delivery, InTACT
3. Richard Hart, Director Solutions Delivery, InTACT
4. Ian Waters, Security Team Leader, InTACT
5. Mr Tom Duncan, Acting Clerk, ACT Legislative Assembly
6. Mr Russell Lutton, Manager, Hansard and Communications, ACT Legislative Assembly
7. Mr Ian Duckworth, Manager, Corporate Services, ACT Legislative Assembly
8. Ms Valeria Szychowska, Assembly IT Manager, ACT Legislative Assembly

Attachment 1 Terms

Active directory

Windows 2000 is the new generation operating system for personal computers and servers based upon the Windows New Technology (Win NT) operating system.

Active Directory (AD) is the name given to the directory service used by Windows 2000 Server. AD controls both who has access rights and who can change access rights to individual network resources such as files, groups, servers and printers. Through the use of AD, different access, logging and control policies can be applied to these resources. This enables enhanced security and easier data management and administration.

AD can be best described by referring to a street directory of a city. A street directory contains suburbs and streets, highlighting which roads are one way, where traffic lights are located and where a street is located on the map in relation to your location. Effectively AD is a map that indicates where you can go and where you cannot. The user of the street directory has more control of their direction in moving to a specific location. AD provides this ability in an IT network environment.

InTACT has recently replaced the previous operating system (Windows NT 4.0) with Windows 2000 and Active Directory.

Organisational unit

An Organisational Unit is a method of organising computer and employee accounts into groups within Active Directory. Using Organisational Units enables selective customisation of the computing environment for employees by department or section.

The set-up of an Organisational Unit can also have restricted access from the rest of the Domain that it resides in. Access can be restricted to direct administration staff— for example, Yellow Team Helpdesk and Central Server Facilities (CSF) staff.

When referring to the street directory analogy, an Organisational Unit is a specific suburb on the map. A suburb is contained within a city (a network domain) but has different planning rules applied.

This diagram below depicts a network structure with a single Organisational Unit under the ACTGOV Domain. The Organisational Unit depicted here can have different security policies implemented from the structure above.