LEGISLATIVE ASSEMBLY OF THE NORTHERN TERRITORY

WRITTEN QUESTION

Mr Bohlin **to** Minister for Business

NTG Information and Communication Technology (ICT) Outsourcing

The NTG Information and Communication Technology (ICT) Outsourcing contract expires in 2010:

(1) What operational procedures are in place in relation to ICT to ensure that all @nt.gov.au (NTG) account holders' electronic (email) and voice communication information is secure from misappropriation.

(2) What operational procedures are in place to identify the inappropriate distribution of information from NTG account holders through ICT, particularly as it relates to material in confidence.

(3) What operational procedures are in place to identify the improper use by NTG account holders of ICT resources, particularly as it relates to accessing inappropriate content or abuse of service.

(4) What security and probity checks are completed on persons within the NTG who may access the electronic and voice communication information and data of NTG account holders.

(5) What security and probity checks are completed on persons working for providers of ICT services to the NT who have access to NTG account holders' electronic and voice communication information.

(6) What physical controls are in place for the security of the storage and transmission of electronic and voice communication.

(7) Has any person been identified distributing electronic communication acquired through the monitoring or surveillance of NTG ICT in a way that breaches the confidentiality of that communication.

(8) Has any person, within NTG or ICT service provider contractor employees been disciplined for the inappropriate access of electronic or voice communication from NTG account holders.

(9) What positions (including numbers of persons, NTG or ICT provider) have access to the NTG electronic and voice communication for the purpose of implementing and monitoring security of the ICT system.

(10) What, if any, additional security practices and activities are proposed for future ICT service delivery.

ANSWER

NOTE

Answers to the ten questions raised give some insight into the layers of security the Northern Territory Government uses to minimise misappropriation of government information and misuse of government electronic services. Business best practice is to minimise making public detail of such security responses.

(1)

Operational procedures are in place to ensure that Northern Territory Government (NTG) user accounts, including email accounts, are only created when authorised by an NTG delegate. User accounts are protected by passwords that are required to be changed every 30 days.

The technology in use for email does not allow a standard NTG account holder to access any email other than their own without the permission of the person concerned or under the authority of their agency chief executive. System administrators have the technical ability to access user email files, but are only allowed to do so in specific circumstances, such as in the course of an investigation authorised by an agency Chief Executive, or while diagnosing and correcting a technical fault.

It is feasible for NTG email accounts to be misappropriated as a result of user login credentials being stolen in “phishing” attacks, where users are tricked into revealing their user id and password. This form of attack is endemic on the internet, and from time to time, a well crafted external email, received by many NTG users, may result in a small number of compromises. Procedures are in place to identify and block these quickly. In general, these attacks do not target NTG information specifically, but are intended to facilitate the distribution of spam.

To protect voice communications against misappropriation, physical security limits access to rooms containing communications equipment. There is no instance where misappropriation of voice communications is suspected to have occurred.

(2)

See answer to Question 1 regarding access by individuals outside the Northern Territory Public Sector (NTPS) or unauthorised personnel within the NTPS. The primary current safeguard against the inappropriate distribution of information by NTPS personnel with authorised access using ICT is the probity, honesty and good intent of NTG Public Sector employees, reinforced by the Code of Conduct. This Code of Conduct together with physical security practices also provides the key safeguards against the inappropriate distribution of hard copy information.

Breaches, if they occur, can be investigated. An investigation can determine if a user inappropriately distributed an IN-CONFIDENCE document to another person via email by reviewing the logs.

Electronic documents are categorised according to their level of security. The authority levels of staff assigned by managers, governs the level of electronic access they can have to this information sufficient to carry out their duties.

(3)

Technical systems are in place to block access to inappropriate content on the internet. Operational procedures are in place to manage those systems.

Access to web sites by all NTG LAN users is filtered. SurfControl, a commercial web filtering product, is used for this purpose for most NTG users. The NT Schools environment uses a different product (Bluecoat) that provides equivalent functionality.

SurfControl contains a list of several million web sites, grouped into categories. A number of these categories are deemed to be inappropriate and so any website classified in those categories is blocked.

The following roles and responsibilities apply:

- Changes to the banned categories list requires the approval of NTG Information Management Committee (NTGIMC).
- Re-categorisation of web sites requires the approval of the ICT Security Unit.
- Exemption from filtering requires the approval of an agency CE.

(4)

As covered in Question 1, NTG staff members do not have the system administration privileges required to access other user's email accounts, electronic data, or voice communications information directly. Access to email accounts and electronic data can be gained only when an investigation is authorised by an agency Chief Executive.

A very small number of the Department of Business and Employment (DBE) staff have access to network monitoring systems that watch and report on network traffic flows, network filtering, network intrusions, virus activity and other aspects of routine network administration.

Access to voice information (such a call intercepts) is not possible except under the provisions of the *Telecommunications Interception Act* (Commonwealth). In practice, if a Chief Executive wishes to have calls intercepted (say, for example, as a result of a complaint about abusive phone calls) then DBE will advise the Chief Executive to make a formal complaint to the police.

There are currently no special security or probity checks completed on the very small number of NTG Public Sector employees who may from time to time have access to the systems mentioned above, or participate in investigations.

(5)

Service provider staff that have privileged access, including system administrators with the technical ability to access NTG account holder's electronic and voice communications information, are required to undergo police and reference checks before they can work in the NTG environment. This is a requirement under the contracts with the service providers

(6)

There are numerous physical controls in place for the security of the storage and transmission of electronic and voice communication. These range from, for example, the security controls against unauthorised access to the Chan Building Data Centre, to the special cages containing communications equipment in NTG occupied buildings.

(7)

No.

(8)

In May 2008 an ex-employee of a service provider caused disruption of the NTG's network. Police prosecutions were levied against the offender who has been tried and convicted.

In the last two years 10 investigations of misuse have been authorised and undertaken. In four cases there was no evidence of inappropriate use, in the three other cases disciplinary action was taken (with two officers subsequently resigning from the NTPS) and the three remaining cases are still under investigation.

(9)

	NTG (Whole of Government)	**Agencies**	**Comms Service Provider**	**Email Service Provider**	**Desktop Service Provider**
Firewalls, NTG Web Filter, Designs.	1 (Approvals, monitoring)		5 (Applies changes, monitoring)		
Telecomms Reports including Security reports	2	10 (Incl Agency IT Managers)	10		
Email systems and related filters.	0			5	
Network monitoring tools (including anti-virus consoles, network traffic flow tracking tools etc)	1-2		5	5	5

Note. The numbers above do not include the Schools environment which has its own outsourcing arrangements for email and desktop services.

(10)

Future outsourcing requirements are currently being developed. Changes to some important security technologies are best put in place at the time of contract transition. DBE is developing technical initiatives including;

- Stronger gateway standards,
- Stronger filtering technologies for spam, viruses and web access.
- Stronger intrusion detection technologies.