Submission No. 68

'yes' OPTUS

26 June 2003

inc 3/6

The Secretary
Joint Committee of Public Accounts & Audit
Parliament House
CANBERRA ACT 2600

Dear Secretary

Optus is pleased to respond to two additional questions on notice requested by members of the Joint Committee of Public Account and Audit for the inquiry into "The Management and Integrity of Electronic Information in the Commonwealth".

1. **Submissions from various Government departments mention staff training designed to raise awareness of privacy and security issues. What training do Optus' staff receive on issues relating to the management and integrity of the Commonwealth's electronic information?**

Security

All Commonwealth Government departments have different security policies that apply to the management and integrity of electronic information that Optus may manage on behalf of the Commonwealth.

Optus supports staff training that raises awareness of security issues when managing electronic information on behalf of the Commonwealth. This includes:

- Providing all Optus staff who manage electronic information on behalf of the Commonwealth copies of security processes and procedures that define their obligations appropriate to the requirements determined by the Commonwealth Department they are working with.

- Requiring Optus staff who manage electronic information on behalf of the Commonwealth obtain the level of security clearance required by a Department. Security clearances. These security clearances are generally assessed and granted by the Commonwealth through the Australian Security Vetting Service (ASVS).

- As is specified for ASVS clearance process, Optus staff who manage electronic information on behalf of the Commonwealth are required to sign the ASVS application to confirm that they understand the obligations and penalties that will be applied if security is breached.

Optus also undertakes annual independent audits of the processes and procedures that have been established for security awareness and training.

Privacy

Optus has privacy obligations under the *Telecommunications Act 1997*. As a result, privacy has been included in staff training programs for many years.

Optus also has obligations under amendments made to the *Privacy Act 1988* and subsequent introduction of the National Privacy Principles (NPPs) and has enhanced its privacy training with new programs implemented for all staff.

There are two key programs in place:

- Induction training - all staff are required to complete an online induction training program at the commencement of employment with Optus. The induction program includes a general module on privacy including an overview of the NPPs.

- General/ongoing training - all existing staff have been required to complete a privacy training program prior to the commencement of the NPPs in December 2001. This online program is available on the Optus Privacy intranet site for ongoing, refresher training as needed.

Both the privacy induction and general training programs are sophisticated online programs which monitor staff participation and include a competency assessment test. This has enabled Optus to ensure that all staff complete the program to a specified 80% pass rate. Staff who fail the assessment are required to repeat the modules.

All staff complete a general module covering key aspects of privacy requirements including security.

2. Social Engineering is the use of deception, influence and persuasion to overcome security measures. This is a potential risk to the privacy and security of electronic data. What action is Optus taking to guard against this potential problem?

Social engineering involves outsiders tricking legitimate company personnel into aiding covert acts such as supplying proprietary information or allowing inappropriate access to systems. Optus agrees that social engineering is a risk to the privacy and security of electronic data.

Optus has implemented numerous policies to protect against these types of attacks. These policies are administered by Optus as well as our contractors and include information release, access approval, password changes, external access and help desk verification processes.

Specific strategies Optus employs to guard against social engineering include:

- Identification of employees and temporary contractors via photo identification, with visitors identified with visitors passes
- Use of security bins to dispose of confidential documents
- Well publicised processes for employees to report violations or suspicious activity
- Ongoing security awareness programs
- Systems intrusion detection / monitoring
- Forced regular password changes

If you have any further queries please contact Michelle Curtis, Manager Government & Community Relations on (02) 9342 6247.

Yours sincerely

David McCulloch
General Manager, Government Affairs