



30 April 2003

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

Dear Secretary

Optus is pleased to respond to two questions on notice made by members of the Joint Committee of Public Account and Audit (the committee), at the 2 April 2003 hearings conducted for the inquiry into "The Management and Integrity of Electronic Information in the Commonwealth".

Comment on Australian Government Use of Information and Communication Technology - a New Governance and Investment Framework

Mr Bob Charles MP requested Optus to provide an opinion on whether the report - *Australian Government Use of Information and Communication Technology - a New Governance and Investment Framework* (the report) prepared by the Public Service Commission in November 2002 - represented a good overall starting point for a strategy for the Commonwealth.

Optus believes that the report is a valuable starting point for the Government to improve the management and integrity of electronic information in the Commonwealth.

Detailed below is how specific recommendations of the report support suggestions for reform that Optus presented in its submission to the inquiry and in our appearance before the committee.

Following this discussion are additional suggestions for reform not contained in the report that Optus believes should be considered by the working groups established by the report.

Endorsed Product Listing (EPL)

Optus suggested to the committee that the EPL listing process be streamlined to reduce the length of time taken for approval and to reduce the cost of registration. We

also recommended that a faster approval process for products - both software and hardware - that have already gained an EPL listing, but have been modified or upgraded, would be of immediate benefit to business and the Commonwealth. Optus notes that the report suggests actions to improve the process for EPL. The report recommends that the ITAG Secure Business Systems Working Group:

"investigate ways and means of improving the process for the EPL, which may include a more proactive approach to endorsement to lower the cost and length of time involved in getting products evaluated and on the EPL". (p.31)

Security Classification Methodology

Optus is concerned that current security classification methodology results in all information being classified to a level demanded by the most valuable information carried over a network. This then requires 'a gold-plated solution' to security of information for questionable benefit.

The report makes a good starting point to addressing this concern by recommending that the Secure Business Systems Working Group should:

"consider an ACSI-type instruction relating to applications development that would require data classification and secure storage issues to be identified and addressed effectively in the design stage." (p.30)

However, Optus believes that the working groups established as a result of the report should also recommend that the security classification guidelines need to give greater consideration to the:

- value of the information being protected,
- efforts that an attacker must undertake to compromise the information, and
- the additional costs associated with encrypting over-classified information.

Optus is also concerned that the security classification guidelines are inflexible in terms of the security facility that must be provided once information has been classified as protected.

As outlined in our submission, it has been Optus' experience, that there is no recognition of the security features of our private secure internet; it is treated as 'untrusted' just like the public internet. In some instances this has led to the implementation of expensive and unnecessary security solutions.

Optus believes that the working groups established as a result of the report should evaluate the barriers to entry for companies who want to provide security services to the Commonwealth, particularly the high cost of establishing a secure facility and the complexity and cost of attaining gateway certification.

Standard Security Guidelines Across Government

Optus notes that the report was concerned about:

"the range of policies, regulations and legislation [that] combine to form the existing governance and financial framework for ICT acquisition, development and management". (p.7)

The report also recommended that:

"in this changing policy and program environment there is a case for a more coherent framework across government". (p.7)

As part of the process to develop a more coherent framework across government, Optus supports an evaluation of the number of inconsistent, inadequate and costly system of security standards between:

- Commonwealth agencies,
- Commonwealth and State and Territory Governments, and
- between all levels of government and business.

Additional Considerations

Optus further submits that the working groups established as a result of the report should consider:

- The establishment of an Australian Standard for security which would be applicable to both the private and public sector at all levels of government. Such a standard could contain the ability to classify information at different levels according to the nature of the data. This would create a 'common terminology' that would give reassurance that information is being treated consistently regardless of whether a Commonwealth agency, a bank or an intermediary providing services for the government is involved.
- Applying security at the application layer as opposed to the network. Given the ubiquitous nature of the internet, applying security at the application layer would enable the transport of data across public networks regardless of the security classification of a particular network.

Protecting Critical Infrastructure

Senator Kate Lundy requested information on *"Optus' involvement in and opinion of the process of protecting critical infrastructure currently being coordinated by the Attorney General's Department"*.

Optus has been involved in both State and Commonwealth Government initiatives aimed at protecting privately owned critical infrastructure.

Our representatives have participated in the following forums convened by the Attorney General's Department's 'Protection of Critical Infrastructure Protection Group' including:

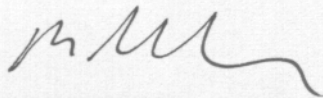
- March 2002 Business/Government Taskforce
- July 2002 Business/Government Taskforce Recommendations briefing
- April 2003 Protection of Critical Infrastructure meeting

Optus representatives also regularly participate in the 'Inter Carrier Critical Infrastructure Advisory Group', established in November 2002 by the NSW Police Force.

Optus supports the establishment of both State and Commonwealth critical infrastructure protection processes.

Optus is very supportive of assistance and guidance provided by all levels of government in the protection of our critical infrastructure.

Yours sincerely,



David McCulloch
General Manager, Government Affairs