Contact officer: Jim Wolfe 02 6274 7611

Dr John Carter (john.carter.reps@aph.gov.au)
Inquiry Secretary
Management & Integrity of Electronic Information in the Commonwealth

Dear Dr Carter

PUBLIC SUBMISSION FOR THE JOINT COMMITTEE OF PUBLIC ACCOUNTS & AUDIT INQUIRY INTO MANAGEMENT & INTEGRITY OF ELECTRONIC INFORMATION IN THE COMMONWEALTH

I am writing on behalf of the Department of Transport and Regional Services (DOTARS) regarding your inquiry into the *Management and Integrity of Electronic Information in the Commonwealth.* While the Department does not wish to make a formal submission, we are happy to provide some information that might be useful background in relation to IT services in the Department.

1. Outsourcing of our IT Services

(a) Transition processes if changing providers:

An audit by Acumen Alliance is currently underway for all agencies in Group 5 to identify the readiness for a transition to another provider and/or to new contractual conditions. This is in preparation for a potential change in provider on, or before, expiry of our current contract with TELSTRA in June 2004. The audit will document key findings of the current environment and make recommendations for remedial actions if necessary.

In addition to the audit, we are currently implementing the UK Government endorsed Information Technology Infrastructure Library (ITIL) processes that will assist us to better manage any future outsourced arrangements with external providers. This work is being done with the full cooperation of TELSTRA.

Other relevant key IT service practices in place include:

- The Department's web hosting is provided by one of two endorsed suppliers that have the required level of secure gateway access for Commonwealth sites; and
- Our network and security practices meet the stringent requirements for use of the FEDLINK network. This endorsement will be officiated shortly.

(b) How do our providers store our back up information:

Information back-ups are completed every night. These are then stored off site by a commercial provider that meets the current Commonwealth security requirements.

(d) Have private sector employees got access to stored confidential and above information:

Appropriate security clearances for access to information are in place for outsourced staff. The DOTARS network access is designed to accommodate information up to protected level classification. Information above this classification is not stored on our network and therefore unavailable to private sector employees. Guidance material on our

Intranet, regular information sheets and seminars are held for Department staff to refresh their knowledge on the importance of maintaining information security standards.

(e) How do we ensure tenders meet Government required security needs?

Every tender and project has a specification that all areas must comply with the Protective Security Manual requirements. Compliance levels are regularly checked by out IT Security adviser and audit regime.

2. IT Security Plan

DOTARS has an established IT Security Plan which is regularly reviewed and is available to staff on our intranet.

Staff have also been educated in IT Security and in the use of the Internet. They have been provided with email usage guidelines. Annually staff agree to abide by these guidelines before being granted log in access to our computer systems.

Screen Savers also are used to remind staff of their obligations in this area.

3. Transfer and storage of electronic information of National Security interest

DOTARS does not store or transfer this level of material over our network as it is only designed to PROTECTED level. Instead, special arrangements outside of our network are in place – such as equipment supplied by specialist Agencies that enable receipt/transfer of highly sensitive information. Overall DOTARS has very little of this level of material.

As a further indication that DOTARS is dedicated to ensuring it manages and maintains the integrity of its electronic information, the Department has independently engaged Acumen Alliance to complete the following:

- A full IT Security review and Risk assessment;
- A Web Development and security audit; and
- An IT Governance audit.

Recommendations from these audits have been accepted and implemented by DOTARS.

Regards

Faye Powell
General Manager
Information Services
Department of Transport and Regional Services.
January 2003