# INQUIRY INTO THE MANAGEMENT AND INTEGRITY OF ELECTRONIC INFORMATION IN THE COMMONWEALTH

## Further Questions for the Commonwealth Ombudsman

**1. Your submission states that sound information management requires that the management and transmission of information be able to be authenticated, secure, robust and to be contextualised. Your submission notes the difficulties in meeting these requirements when working with electronic records.**

***Would you expand on these difficulties?***

Before computers a manual file or folder was both the record keeping point and also the method of storage. For example: A file would come to an employee's desk with a note attached, the person would respond with another note, and everything would be put in the file and forwarded on or returned to a filing cabinet. The file was the means to both distribute and store records.

The Ombudsman's office uses e-mail, a case management database and the Internet, accessed through desktop personal computers also used for word processing and Internet searches. As a result, it has moved away from paper-based records management, so that the only records held on the paper file will be those which are held only in paper form and printed versions of electronic records considered to be of significance to the file. Many transient records – for example, routine e-mails and superseded drafts – will be discarded. Work practices and the referencing of paper and electronic records to electronic case management and administrative files assist in coordinating availability and use of documents.

There remain difficult technical issues in bringing about seamless document movement between various desktop applications, server-based applications and databases and manual storage. These problems are significant for an agency with limited resources. The availability of electronic documents to different users can create problems in identifying which is the authoritative version and in maintaining document security.

***Can you suggest a solution to this problem?***

Ombudsman's office staff can place electronic copies of Word documents and e-mails onto the case management database. The case management system also enables paper records to be related to the case management database so that investigation staff can identify and locate those paper records for use in an investigation. These facilities were purpose built for the office's purposes, as most "off-the-shelf" products would not enable record sharing.

The other area of concern is the sharing of a document in electronic form can result in duplication and modifications from the original. This results in authentication and security being an issue. Original documents need to be maintained securely and any updates or modification need to be tracked.

**2. Your submission states that electronic data needs to be linked and cross-referenced with the paper data so that all data can be comprehensively retrieved. How might this be achieved?**

This question has been addressed in the response to Question 1. The principle of linking between the electronic environment and the paper environments by a common reference number as well as title information addresses our needs without going to an expensive records management application. This enables electronic documents created by staff to be classified consistently throughout the office, and offers a powerful search facility to help retrieve documents more easily. Investigators now have quick access to case information. Staff can find a document as well as cases wherever it is stored, and they can identify its relationship with other documents.

**Social Engineering**

**3. 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 being taken to guard against this potential problem?**

It is impossible to prevent attempts to overcome security systems aimed at ensuring the integrity of data. What organisations can do is to:

- foster a workplace where staff are alert to threats to data security;
- develop information technology systems where improper access is prevented if possible and detected and acted upon if not.

The Ombudsman's office aims to achieve these goals through staff training, the encouragement of sound work practices and the ability to track access to a record. Problems can also be identified and rectified through audit trails.

**Archival Integrity**

**4. What action is the Office of the Commonwealth Ombudsman taking to ensure the long-term archival integrity of its data?**

When electronic information, including data structure, is backed up, it is maintained in a format accessible with the same technology as is used for the

database. When the office changes it technology, we propose to ensure that future changes will be applied to the information already stored.

**Additional Correction to proceedings Tuesday 1st April 2003**

***Mr Plibersek asked Mr Taylor about the nature of network traffic between the centralised database and the state offices.***

*A reference was given that the Ombudsman's office operates connectivity to regional offices via Virtual Networking via the Internet.*

**Additional Information:** We do not use the Internet (virtual networking) or phone lines for case management communications. Our wide area network consists of a private frame relay network ranging from 128k bps to 64k bps. This network has had independent security audits applied and is considered suitable for the nature of traffic. The Ombudsman office uses a private TCP/IP (class C) network. The nature of network traffic for case management is HTTP (browser) service between a central Oracle database and desktop PC workstations. A central web server within the Canberra office controls this traffic.

The office also operates a secure firewall and content filtering to the Internet. The Internet is only used for external mail and browse connectivity and hosting our external web site and online complaint handling.

We would be happy to provide a demonstration of our IT environment, if the Committee was interested.