COMMONWEALTH OMBUDSMAN

Complaints: 1300 362 072
Tel: (02) 6276 0111
Fax: (02) 6249 7829
www.ombudsman.gov.au
Level 6, 1 Farrell Place
Canberra ACT 2600
Australia
GPO Box 442
Canberra ACT 2601

13 January 2003

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

Dear Ms Kerley

I refer to your letter of 28 October 2002 inviting a submission to the Committee's inquiry into the management and integrity of electronic information in the Commonwealth and to the e-mail exchange between Dr Carter and Mr Bluck about the timing of our submission.

I have attached my office's submission. My officers are available to discuss the submission or provide further information if requested; my contact for this matter is Mr John Taylor, Senior Assistant Ombudsman (Professional Standards and Administration) who can be contacted at john.taylor@comb.gov.au

Yours sincerely

R N McLeod
Commonwealth Ombudsman

SUBMISSION TO
PARLIAMENTARY JOINT COMMITTEE
OF PUBLIC ACCOUNTS AND AUDIT
INQUIRY INTO
MANAGEMENT OF ELECTRONIC INFORMATION IN THE COMMONWEALTH
SUBMISSION BY THE OFFICE OF THE COMMONWEALTH OMBUDSMAN

This submission will address the Committee's Terms of Reference after setting out how the office of the Commonwealth Ombudsman manages the electronic information it holds and commenting on information management practices more generally.

Background

The Commonwealth Ombudsman investigates the administrative actions of Commonwealth agencies, either following a complaint or on the Ombudsman's own motion. Complaints may be made orally (in person or by telephone), in writing or through the Ombudsman's internet site. The Ombudsman has extensive powers to require information to be provided, but in practice most agencies provide information relevant to an investigation without being compelled to do so. Investigations are conducted in private and as the Ombudsman sees fit. Information can be disclosed only by the Ombudsman in a report or in the public interest by the Ombudsman or a few delegates.

The Ombudsman is also the Defence Force Ombudsman, the Taxation Ombudsman and, under an arrangement with the ACT, the ACT Ombudsman. The Ombudsman also has a statutory inspection role in relation to telecommunications interceptions and controlled operations conducted by Commonwealth law enforcement agencies.

The Ombudsman has a staff of about 80, spread between a national office in Canberra and regional offices in all states and the Northern Territory. Staff who conduct investigations do so under delegations issued by the Ombudsman. Each year, the Ombudsman's office receives about 20,000 complaints and investigates about 30% of them; in the remaining cases, a discretion not to investigate is exercised, usually because there is another avenue available to the complainant. As well, the office receives about 12,000 other inquiries.

Information held

The bulk of information held by the Ombudsman's office comprises information provided by complainants and by agencies in relation to investigations. This information is usually personal (but sometimes business-related) and is often highly sensitive. The office generates further sensitive material in the course of its analysis and investigation of administrative actions.

The office also holds information relating to:

- inspections of law enforcement records;
- its own management and administration; and
- policy development in the office and throughout government more generally, including in relation to the Ombudsman's role as a member of the Administrative Review Council.

The Ombudsman and staff are subject to an array of secrecy and confidentiality provisions in legislation administered by the Ombudsman and in legislation relevant to particular kinds of information.

IT in the Ombudsman's office

The Ombudsman's office maintains a national information technology network which permits staff to:

- access and update a national complaint management database (Combi). This information is often supplemented by hard-copy material (for example, where a complaint is made in writing and where an investigation is likely to take some time);
- receive and send e-mail within the network and externally. Typical uses would be to inform an agency of a complaint and seek and obtain responses from it to issues raised by the complaint or to consult another staff member who may have specialised knowledge about the relevant area of administration;
- access internet services, subject to guidelines and controls, and an intranet service which contains information relevant to staff and the Ombudsman's functions; and
- carry out administrative functions related to their work.

The office's model is centralised, with different access for different types of users and logging of access to records, changes and destruction. Electronic records are linked, where appropriate, to the relevant hard copy holding. Records are regularly backed up and strategies are in place to provide high speed and efficient access to records for all the Ombudsman's dispersed staff, subject to their level of access.

The Ombudsman's office registers on its registry system all new paper correspondence it receives so that there can be connections made between a paper file, electronic records and the new item which enable the matter to be referred to the appropriate staff member.

It would be much more difficult for the Ombudsman's staff to carry out their work effectively without access to information technology. Technology provides them with the capacity to receive and record complaints; to search for other complaint records containing similar features (eg complainant, agency or issue); to conduct

legal and other research as part of investigations; to ensure reasonable consistency of approach between similar cases and to communicate their decisions. The office often creates hard copies of records of more enduring value to retain on files.

The Ombudsman has a website (http://www.ombudsman.gov.au) containing information about the office, publications and links to other sites. Members of the public can make complaints through the website. The office maintains a firewall between the external website and the internal corporate network. The objects of the firewall include preventing external access to secure information and preventing virus or other attacks compromising the internal network.

Inevitably, some information is passed over the external network:

- when a complaint is made through the website; and
- when an investigator consults an agency or responds to a complainant by e-mail.

Information security in the Ombudsman's office

The Ombudsman's office has a "clean desk" policy requiring staff to put away into lockable cabinets files and documents related to their current work. Non-current files are held in a secure registry. Additional copies of records and items of transient value only are either shredded or disposed of through a secure waste facility.

Access to the Ombudsman's corporate network is controlled by individual passwords which must be changed at least quarterly. Staff are divided into user groups with common needs for information, to preclude browsing into the work of other areas. Some law enforcement information held electronically is specially protected and is accessible only by a limited number of staff with a need to know. Staff are required to acquaint themselves with and apply the office policy on the use of Information Technology Services. The office acts to protect its internal network from malicious or damaging material.

Staff are required to comply with relevant legislation (which prevents the making of personal records of investigations and the unnecessary disclosure of information) and with office instructions intended to ensure that the privacy of complainants is protected.

Information management generally

The Commonwealth sector holds a very large amount of information for proper administrative purposes such as collecting taxes and charges, making contracts, issuing visae, paying pensions and benefits, regulating areas of the economy, law enforcement and the employment of its own staff. The level of detail at which Australian legislation typically operates will often require a decision-maker to

become informed about a great number of matters before making a decision affecting an individual or business.

There are, however, limits on:

- the information an agency may solicit or demand for its purposes;
- disclosure of information by agencies and their staff members; and
- transfer of personal information between arms of the Commonwealth.

These factors require that information held by the Commonwealth be properly managed.

The requirements of sound information management in a general sense appear to be that the management and transmission of information be:

- able to be authenticated – that is, a person receiving information should know where it is from and where it is being sent and the weight to be accorded to the document;
- secure – only those with a need to know and a proper right to know should be able to access the information;
- robust against organisational and technological change; and
- capable of contextualisation so that the environment in which a record was made can be considered in relation to the record.

With paper records, it is likely that problems will arise less often than they can with electronic records. A paper record will be able to be read while ever there is a person with the language skills to do so. It will usually exist as part of a file or other ordered holding of related information. It will usually be signed by its originator and addressed to its recipient. If copies are made, it will usually be clear which version of the document was the original. On the other hand, problems do occur and the occasional episodes where sensitive records are found in public places are demonstrations.

On the other hand, it will often be impossible for a recipient without special skills and access to the relevant computer systems to detect whether a document represents the final or settled form or a draft or to be confident that the document comes from the person identified as its author or is being sent only to the addressee. It will usually be possible for an electronic version of a document to be copied and changed without detection and it may be difficult to ensure that all related records are accessible to establish context, especially if they exist in different forms. Usable access to a record can be lost, not only if there is an organisational change, but also if technology changes without adequate preparation for transition.

An inevitable consequence of the explosion in information technology is that more information is held by agencies, companies and individuals. An interchange that may previously have been conducted orally is now more likely to have been recorded in e-mail. Overtaken drafts and comments can often be

summoned from backup, even if the hard copies of all but the final version have been discarded.

These extra holdings can create technical problems of storage and access; as well, there is probably a lack of knowledge among officials generally about the documents their agency might store electronically. That can become a problem for agencies when information is sought:

- under Freedom of Information legislation;
- as part of a litigation process; or
- for the purposes of an administrative inquiry.

(It would not often be the case that potentially damaging documents are not deliberately hidden in electronic form to prevent damage, merely that it is far more likely that those responding to a request or demand may not think to seek out electronic records).

Linking electronic records to paper files

The electronic data needs to be linked and cross-referenced with the paper data so that if data about a person or matter is required, all data can be comprehensively retrieved.

- It follows from this that it is important that electronic correspondence, internal and external, and notes which would have in the past formed part of the official record, be appropriately stored as part of the comprehensive records of an agency.

Ability to audit access

In my view, it is important for government agencies to have an effective and timely means of auditing access to electronic holdings.

This will ensure that persons conducting improper accessing of data may be tracked and identified. An auditable system should include:

- individual logon identification access limited to only those areas of data relevant to the official's duties; and
- onscreen warnings regarding the need to protect data and relevant penalties for breaches.

Terms of Reference

<u>Privacy, confidentiality and integrity of the Commonwealth's electronic data</u>

Commonwealth agencies should have systems in place to enable them to be able to assert confidently that they hold only that information which is necessary for their proper purposes and that the information is protected from unwarranted access or intrusion. Public confidence in Commonwealth agencies depends on

agencies treating information provided to them with proper respect for the person, business or activity to whom or which it relates.

The standard maintained must be high, but arguably need not be uniform. Any class of information may be sensitive in some cases - for example, the address of most people can be ascertained from the telephone directory, but for a variety of good reasons, many people choose or feel obliged to have silent telephone numbers. But some information is inherently more sensitive (for example, information about health, domestic arrangements, personal finances and business innovation) and any information may be more sensitive in one context rather than another.

How an agency goes about ensuring that its holding of information is sufficiently accurate, up to date and relevant for its proper purposes will be a matter for each Commonwealth agency. It may be necessary, for example, for an agency to retain financial information obtained from a person or business for an extended period to meet audit requirements or to deal with appeals and reviews.

Management and security of electronic data transmitted by Commonwealth agencies

Commonwealth agencies should be confident that their transmission of information is secure, lawful and capable of authentication. They should be able to ensure themselves, their Ministers and the Parliament that information is not disclosed when it should not be, that it is difficult or impossible for impostors to forge information and claim that it came from an agency and that information they provide on public websites is up to date and accurate.

If an agency encourages its client group to communicate electronically, it should take the trouble to minimise the risk of damage. If it cannot be certain that a public network is sufficiently secure for the reasonable conduct of some or all of its functions, it should not use it. Again, however, these decisions need to be made by agencies having regard to their requirements and the needs of their client group.

An agency should be able, through user logs or otherwise, to ascertain who has accessed and transmitted information.

Management and security of the Commonwealth's electronic information stored on centralised computer architecture and in distributed networks

The office of the Ombudsman has found that its needs are best met by a centralised system with remote access. The system is not accessible from outside the office, although there is a separate website.

A centralised system makes backup and consistency in information holdings easier to secure. It may be less achievable where very large amounts of information are involved, or where there are other reasons for localised or distributed holding of information. As well, it can be difficult to ensure consistent and reliable response times.

Adequacy of the current legislative and guidance framework

The current system is generally capable of operating reasonably well, although the experience of the Ombudsman's office suggests that agencies do not always look to their electronic records when they should. With the inevitable changes in agency personnel and organisational structure, and the decreased availability of staff resources to manage paper filing systems, electronic records should be among the first resources checked for the light they can throw on a matter.

In terms of guidance, the National Archives of Australia has useful collection of information available on its website (http://www.naa.gov.au/recordkeeping/er).