COMMONWEALTH OF AUSTRALIA

Audit and Fraud Control
GPO Box 9848, Canberra ACT 2601
Telephone: (02) 6289 7736 Fax: (02) 6289 8581
ABN 83 605 426 759

Commonwealth Department of Health and Ageing

Ref: 2003/008528

Mr Tas Luttrell
Sectional Committee Secretary
Joint Committee of Public Accounts and Audit
Parliament House
CANBERRA ACT 2600

Dear Mr Luttrell

INQUIRY INTO MANAGEMENT AND INTEGRITY OF ELECTRONIC INFORMATION IN THE COMMONWEALTH

I refer to your letter of 29 April 2003 to Dr Wooding providing for the Department's response some additional questions arising from the public hearing on 31 March 2003.

Please find attached the Department's responses to the questions.

Yours sincerely

Signed and authorised for transmission by email by

Stephen Dellar
Assistant Secretary
Audit & Fraud Control Branch

20 May 2003

ATTACHMENT

DEPARTMENT OF HEALTH AND AGEING
RESPONSES TO ADDITIONAL QUESTIONS RELATING TO JCPAA INQUIRY IN THE MAMAGEMENT AND INTEGRITY OF ELECTRONIC INFORMATION IN THE COMMONWEALTH

Question 1 - Privacy: Your submission quotes an independent review which states that DoHA has a strong implicit culture of privacy protection. ***How was this culture built and how is it maintained?***

Departmental Response

The independent review quoted above found that the Department of Health and Ageing's (DoHA) strong implicit culture of privacy protection flows partly from the secrecy and confidentiality provisions applying to DoHA and that there is a high culture of compliance at branch level generated by professional experience, corporate memory and a recognition of the importance of ensuring that personal and confidential information is kept secure. The review further concluded that, at a senior level, a high degree of privacy/confidentiality awareness exists.

DoHA's culture of privacy compliance has also been facilitated through the actions of DoHA's Legal Services Branch, which has for a long time provided internal training in the Department's privacy obligations.

DoHA's privacy culture has been further facilitated through a Memorandum of Understanding for the previous two years with the Office of the Federal Privacy Commissioner (OFPC) which has enabled DoHA to seek extensive OFPC input into DoHA policy development.

DoHA's culture of privacy protection is currently being maintained and enhanced through:

- the formation of a dedicated Health Privacy Section, with responsibility for driving national health privacy policy and maintaining and enhancing the Department's internal privacy framework;
- the appointment of a Privacy Contact Officer, who is responsible for continually developing and improving systems to ensure privacy compliance within the Department;
- the establishment of a Privacy Officers' Network, consisting of representatives from every division and State office of the Department;
- the production and dissemination of a DoHA Privacy Manual, which sets out the Department's privacy obligations in plain English;
- the review and enhancement of Departmental privacy guidelines and procedures;
- the review and enhancement of training programs within the Department;
- the production of communication tools designed to heighten awareness of privacy within the Department;
- the establishment of a system for monitoring and reporting privacy incidents;

- the review of contracting guidelines to ensure privacy compliance by contracted external parties; and
- the development and dissemination of a Governing Register, a plain English guide for Department staff seeking a precis of relevant legislation, directives, standards and guidelines regarding privacy protection.

Question 2 - Social Engineering: 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, but is not mentioned in the DoHA submission. ***What action is being taken to guard against this potential problem?***

Departmental Response

As well as the measures outlined in the response to the previous question on privacy, the security awareness briefing provided to new starters covers responsibilities and risks related to deception, influence and persuasion.

Question 3 - Disaster Recovery: A potential threat to the integrity of the Commonwealth's electronic data is physical disruption caused by an earthquake or fire. ***Would you outline for the Committee DoHA's disaster recovery plan?***

Departmental Response

In relation to the integrity of the Commonwealth's electronic data, back-up tapes are stored off-site. Also spare computer infrastructure is kept available to bring critical services back on-line in the event of such physical disruption.

Question 4 - Archival Integrity: ***What action is being taken to ensure the long-term archival integrity of stored data?***

Departmental Response

The Department is progressing with implementation of DIRKS (Designing and Implementing RecordKeeping Systems) which is the standards-based methodology developed by the National Archives of Australia for agencies to use in improving recordkeeping and information management practices and developing new recordkeeping systems. The Department has upgraded policy for the major record keeping requirements of the Department including archival strategies for the long-term integrity of stored records.

Also, the Department has arrangements in place for the storage and safe keeping of all departmental data held on IT systems. The arrangements include:

- daily backups of LAN and midrange systems to the mainframe
- daily backups of the mainframe to tape
- weekly back ups of LAN and midrange systems to the mainframe
- weekly back ups of the mainframe to tape
- secure off-site storage of back-up tapes.