Department of Employment and Workplace Relations

National Office

GPO Box 9879 CANBERRA ACT 2601

19 May 2003

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

Dear Tas Luttrell

Inquiry into Management and Integrity of Electronic Information in the Commonwealth

I refer to your letters dated 10 April and 29 April 2003.

Thank you for the opportunity to consider the transcript of the evidence taken by the Joint Committee of Public Accounts and Audit on 31 March 2003.

I have no suggestion by way of correction of the transcript.

I attach the questions raised by the Committee and the Department's responses.

I have no further or other material to submit to the Committee and I thank the Committee for the opportunity to assist its deliberations.

Yours sincerely

John Burston
Chief Information Officer

Transcript, 31 March 2003, page 59

1. Your submission states that the Department of Employment and Workplace Relations fully investigates all security complaints by job seekers and acts to ensure that the security of their personal information is not compromised.

- Would you advise the Committee of any complaints that have been received from job seekers and the action that DEWR has taken in response?

The Job Network Code of Conduct outlines the services that job seekers can expect to receive and the manner in which they should be delivered. It is widely circulated. One of the five principles addresses privacy and confidentiality. If job seekers are not satisfied with the services they receive, they are encouraged to contact their provider, and, if they cannot do so, or are unhappy with the outcome, they may contact the department's Customer Service Line.

The Customer Service Line (1800 805 260) records all complaints including complaints about privacy or confidentiality issues. The Department monitors complaints and where serious complaints arise Contract Managers and the Risk Assessment team are notified. Complaints are also used as triggers for quality audits. In addition, when visiting sites, Contract Managers are required to monitor the Provider's procedures for meeting privacy requirements including matters such as adequacy of the Provider's interview facilities and security of record keeping.

For the period from 1 January 2002 to 31 December 2002, 17,907 calls were registered through the Customer Service Line, of which 7,939 were complaints about Job Network. Out of the 7,939, 103 were about privacy matters, and 83 of these were from job seekers. Generally, job seekers complain that a Job Network member or that Centrelink has breached their privacy. Complaints resolved on the spot are usually relate to concerns about the level of information requested by Job Network providers, such as Date of Birth, educational qualifications or work experience. Complaints that require further investigation usually relate to allegations that a Job Network member has discussed personal issues with another person, or a potential employer, without prior agreement from the job seeker. In such instances the Job Network member is reminded of the necessity to ensure that privacy is maintained in future business transactions.

Since 20 September 1999 there have been three complaints from job seekers received through the Privacy Commissioner. In relation to the first, a breach of privacy had occurred, and the Job Network member concerned (which will not be a Job Network member after 30 June 2003) apologised in writing. In relation to the second, the Director of Public Prosecutions determined that the public interest did not warrant the prosecution of the staff member concerned, but sent that individual (who, it is understood, left that employment) a warning letter. The third was made on 6 May 2003 and so is still under investigation by the Department.

- Has any of these breaches led to suspension of access for staff members of any Job Network provider, or termination of a Job Network provider's contract?

No.

Transcript, 31 March 2003, page 60
2. How many different Job Network providers does the Department of Employment and Workplace Relations have under contract?

On 6 May 2003 the Minister for Employment Services announced the licensing of 375 Job Placement organisations, in addition to the 144 Job Network, Harvest Labour and NEIS providers already announced, as providers of services from 1 July 2003.

Transcript, 31 March 2003, page 61
3. Has the Department of Employment and Workplace Relations found any breaches of IT access rules and constraints by Job Network providers?

There have been four incidents over the past year where employees of Job Network members have shared their computer-access passwords. These employees were counselled.

Transcript, 31 March 2003, page 62
4. Has the Department of Employment and Workplace Relations found any instances of inappropriate access by employees of Job Network providers?

There have been two instances of inappropriate access by employees of Job Network providers.

Privacy
1. Your submission makes several references to the Privacy Act 1988 and the Office of the Privacy Commissioner.
- What interactions do you have with the Office of the Privacy Commissioner?

The Litigation and Administrative Law Team (L&A Team) in Corporate liaises with the Privacy Commissioner about matters of concern and seeks clarification and advice about privacy issues as and when they arise.

The team leader of the L&A Team is the Privacy Contact Officer within the department, and as such is the first point of contact for any queries from the Privacy Commissioner.

The Team Leader, as the Privacy Contact officer, participates in the Privacy Contact Officers' Forum which meets regularly to discuss current issues and developments relating to privacy.

Social Engineering
2. 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 your submission.
- What action is being taken to guard against this potential problem?

While the potential impact of successful social engineering is not disputed it does not have the same likelihood as internal fraud or scripted hacking attempts. The main area at risk from social engineering is the IT Service Desk which is called by users experiencing problems such as a forgotten password. This could be facilitated through publicly available information on the Intranet, in departmental or Commonwealth publications or from the switchboard. The aim is assumed to be to access electronic data as someone other than themselves.

The IT Service Desk seeks to confirm a person's identity by asking a question based on stored data about that person. The IT Service Desk, in processing access requests, telephones the person concerned and seeks to talk to them directly.

With the deployment of smartcards in the next financial year it will be not only necessary to know someone's name and their password, it will also be necessary physically to hold the person's access card as well.

Disaster Recovery

3. A potential threat to the integrity of the Commonwealth's electronic data is the physical disruption cause by an earthquake or fire.

- Would you brief the Committee on DEWR's disaster recovery plan?

All production servers are housed in a purpose built IT facility at Bruce, shared with the ATO and DEST. All production data has a back up copy held in a purpose built facility owned and maintained under contract by SecureNet.

The risk of the destruction of Bruce is less than the risk of the destruction of, or disruption to, the main DEWR office campus. This is particularly the case in terms of earthquake or fire. Business continuity in the advent of the loss of Bruce would entail manual processing (at an obvious reduced level of service) while the IT systems were rebuilt according to a national priority (noting that DEWR is not the only tenant at Bruce and that there are other agencies located close to the DEWR office campus).

The Department is currently reviewing its Business Continuity Management and this will provide critical input into the Department's IT Service Continuity Management process which is being developed in accordance with industry best practice. It is the ITSCM process that results in the production of recovery plans.

Archival Integrity

4. What action is DEWR taking to ensure the long-term archival integrity of its data?

DEWR has automated processes in place to ensure that all relevant data is archived according to specified business rules for the relevant retention period. These arrangements are embedded in the design of each system