Department of Employment and Workplace Relations

National Office

GPO Box 9879 CANBERRA ACT 2601

Ms Margot Kerley
Secretary
Joint Committee of Public Accounts and Audit
Parliament House
CANBERRA ACT 2600

Dear Ms Kerley

JOINT COMMITTEE OF PUBLIC ACCOUNTS AND AUDIT:
INQUIRY INTO THE MANAGEMENT AND INTEGRITY OF ELECTRONIC INFORMATION IN THE COMMONWEALTH

I refer to your letter of 28 October 2002, inviting my department to provide a written submission to the above inquiry.

The department's submission is enclosed.

Yours sincerely

(signed)

John Burston
Chief Information Officer
18 December 2002

SUBMISSION PREPARED BY THE DEPARTMENT OF EMPLOYMENT AND WORKPLACE RELATIONS TO THE JOINT COMMITTEE OF PUBLIC ACCOUNTS AND AUDIT

MANAGEMENT AND INTEGRITY OF ELECTRONIC INFORMATION IN THE COMMONWEALTH

DECEMBER 2002

TERMS OF REFERENCE

The Committee shall inquire into and report on the potential risks concerning the management and integrity of the Commonwealth's electronic information.

The Commonwealth collects, processes and stores a vast amount of private and confidential data about Australians. This information is held by various Commonwealth agencies and private bodies acting on behalf of the Commonwealth. For example, the Australian Taxation Office keeps taxpayer records, the Australian Electoral Commission keeps electoral roll information and Centrerlink keeps social security, family and health information. The Committee is concerned that the Commonwealth's electronic information is kept securely and in a manner that ensures its accuracy.

In conducting its inquiry the Committee will consider:

- the privacy, confidentiality and integrity of the Commonwealth's electronic data;
- the management and security of electronic information transmitted by Commonwealth agencies;
- the management and security of the Commonwealth's electronic information stored on centralised computer architecture and in distributed networks; and
- the adequacy of the current legislative and guidance framework.

MANAGEMENT AND INTEGRITY OF ELECTRONIC INFORMATION IN THE COMMONWEALTH

Current legislative and guidance framework

The Commonwealth *Privacy Act 1988*, amended by the *Privacy Amendment (Private Sector) Act 2000*, applies to the Commonwealth public sector and its Contracted Service Providers in respect of personal information collected by public service departments or their Contracted Providers who deliver services for or on behalf of Commonwealth public sector departments.

The amendments to the Privacy Act require all government agencies to bind their Contracted Service Providers to privacy and confidentiality clauses to protect personal information, while at the same time the *Privacy Amendment (Private Sector) Act 2000* binds private sector providers to manage personal information, particularly sensitive personal information, in accordance with the legislation.

While the Privacy Act contains no penalties against unauthorised use and disclosure of personal information collected and held in government agencies, the *Crimes Act 1914* and the *Public Service Act 1999 and its Regulations* contain penalties which vary from fine to dismissal for unauthorised use and disclosure of any information, personal or confidential, held by government agencies.

Guidance on protection of both personal and confidential information is provided in the Commonwealth Protective Security Manual and by the Office of the Privacy Commissioner which has issued a number of guidelines on protection of personal information. The Commissioner's Guidelines can be accessed on www.privacy.gov.au. These Guidelines include protection of personal information collected across the Internet. The Department of Employment and Workplace Relations (DEWR) periodically audits its web sites to ensure compliance with the information management principles set out in the Guidelines.

Privacy, confidentiality and integrity of electronic data

DEWR collects and keeps records of certain personal and confidential information about its customers, its suppliers and its contracted providers.

In collecting, storing and maintaining personal information DEWR operates in accordance with the Information Privacy Principles (IPPs) set out in section 14 of the *Privacy Act 1988*. These Principles govern how the department collects, stores, uses and discloses personal information.

There a number of measures required to ensure the security of personal and confidential information DEWR collects and holds. These are:

- security measures;
- utilising advances in technology to assist customer choice in protecting their information; and
- having established practices in place which are known and understood by departmental staff.

The department regularly trains staff in privacy awareness and in dealing with confidential information and provides advice to staff in the management of personal information. Its procedures manuals dealing with the management of personal and confidential information are available on the department's intranet to all staff.

Since May 1998, DEWR has outsourced the delivery of employment services to commercial entities collectively referred to as Job Network Members (JNM). An intrinsic part of delivering Job Network and other employment services to unemployed Australians is for the Job Network Members to access details of unemployed people through DEWR's Integrated Employment System (IES) computer system.

Jobseeker data is captured by Centrelink under contract on behalf of DEWR. It is keyed into IES using a dedicated closed network connection which encrypts the data.

IES is a mainframe computer system that stores data in a DB2 database - the data is stored in clear text format. Access to this data is controlled by a security product called ACF2. This product has been on the Defence Signals Directorate's (DSD's) Evaluated Product List (EPL) and is considered a 'best of breed' for mainframe security. ACF2 provides both the authentication and authorization function for DEWR.

DEWR's employment services contracts, developed in conjunction with the Attorney-General's Department and the Privacy Commissioner, contain privacy and confidentiality clauses which bind its Contracted Service Providers to observe the Information Privacy Principles and certain National Privacy Principles contained in Schedule 3 to the *Privacy Amendment (Private Sector) Act 2000*. DEWR was a lead department in amending its contracts to reflect the changes to the *Privacy Act 1988*.

The Contracts also contain security provisions which require providers to adhere to stringent security measures to protect data collected and held electronically. The contracts make provision for the Auditor-General and the Commonwealth Privacy Commissioner to audit security and privacy practices employed by the contractor. Indeed DEWR was a model department in having the Privacy Commissioner audit its Contracted providers in advance of the amendments to the Privacy Act.

Contracted Service Providers are required by the terms of the contracts to observe Record Rules attached to the contracts which govern the management of personal information collected for the purposes of the contract, whether in paper or electronic form; to provide notices to job seekers about the use and disclosure practices in relation to personal information collected from them and to train their staff in dealing with personal and confidential information. Furthermore, Contracted Service Providers are required to have their staff sign Deeds of Confidentiality which remind them of their obligations to protect personal and confidential information obtained as part of the provision of services to DEWR.

To assist Contracted Service Providers meet their privacy obligations, DEWR has provided all contracted providers with a video and associated training material dealing with the Privacy Principles in the *Privacy Act 1988*.

DEWR monitors access by staff and Contracted Service Providers to DEWR's employment systems which hold jobseeker records. It regularly checks the browse logs of those systems to ensure that only authorised access has occurred. In addition, where jobseekers believe the security of their information has been breached DEWR fully investigates all complaints and takes action to ensure that security of the personal information is not compromised. The Employment Services Contracts provide for suspension of access of Providers' staff found to be in breach of the Privacy Act. This can, in very serious cases, lead to termination of the contract.

In relation to the management of confidential information, DEWR's contracts protect such information from unauthorised access or disclosure. Access to confidential information, which may include commercially sensitive information about the department's providers, is dealt with under the provisions of the *Freedom of Information Act 1982*, which provides for exemption from disclosure for such material where it meets the criteria set out by the legislation.

DEWR invests considerable resources in technological measures to ensure security of all information held electronically. The department's Internal Audit Annual Work Plan provides for review of systems development to ensure appropriate standards are met.

DEWRs strategic direction has been to lead the way in delivering information using the Internet. DEWR's Internet presence is protected by a DSD certified Internet Gateway. This includes the firewall itself, intrusion detection systems, vulnerability analysis and incident response. Procedures and documentation to support these facilities are also maintained. Certification is to the 'Protected' level.

Safeguarding confidentiality of data is particularly relevant where employment services are being delivered by JNMs in more than 2000 sites across Australia. The broad distribution of Job Network Member sites militates against extending DEWR's dedicated connection to Centrelink. Transmission of Jobseeker details across the Internet requires encryption/decryption at each end; and requires DEWR to have strong firewall security controls. DEWR uses industry standard 128bit encryption of all information that is accessed by JNMs.

JNMs currently have the option of using an older Business To Business (B2B) facility to download jobseeker personal details into their own computer systems. DEWR has announced the cessation of this facility from the start of the third Job Network market on 1 July 2003. DEWR is further strengthening technology controls on the privacy of jobseeker data by replacing the standard internet browser as the means by which JNMs view jobseeker details with a leading edge "smart client" facility. The smart client will enable DEWR to implement access controls over sensitive data that it publishes to JNMs. Specifically, DEWR can tag data items to prevent them from being copied or printed from the PC screen.

Summary

Commonwealth departments cannot simply rely on legislation to protect the information they hold. Effective information management and protection is a combination of:

- sound privacy policies;
- privacy awareness training of all staff and in particular new recruits;
- contracts which contain sound privacy and confidentiality clauses and which ensure that staff of persons contracted by the department have signed confidentiality agreements in relation to information protection;
- risk analyses of threats to sources of information;
- documentation of security controls;
- development of technological systems which protect information;
- development of systems which allow customers choices in what information held electronically is to be protected and how it can be protected; and
- technological measures such as encryption of information before it is transmitted across the Internet.