ATTORNEY-GENERAL'S DEPARTMENT

Information & Security Law Division

02/10616

Mr T Luttrell
Principal Research Officer
Joint Committee of Public Accounts and Audit
Parliament House
CANBERRA ACT 2600

Dear Mr Luttrell

**INQUIRY INTO THE MANAGEMENT AND INTEGRITY OF ELECTRONIC INFORMATION IN THE COMMONWEALTH.**

Thank you for your letter of 29 April 2003, seeking further information on issues not fully covered by the Committee when it was examining witnesses from the Attorney-General's Department on 1 April. I take this opportunity to also respond to the two questions on notice arising from that hearing.

Turning to the issues you raise, I offer the following responses:-

<u>Question 1) Legislative Framework</u>

As the Attorney-General's portfolio does not have responsibility for the *Archives Act 1983*, there is little I could say about its adequacy today. As regards the *Privacy Act 1988*, I have looked again at the answer I provided to Senator Lundy's question on this aspect (Hansard – JCPAA of 1 April 2003, PA 136 and 7) and I would not add to those remarks.

<u>Question 2) Vetting Procedures</u>

Although statistics such as the 2002 Computer Crime Survey show a decline in attacks by trusted insiders, the Commonwealth is aware of the harm that can be done to an agency's information and/or reputation by unscrupulous Information Technology (IT) staff. They have virtual keys to the virtual locks securing the IT system, giving them access to everything on that system.

Some agencies have sought to redress this problem and developed their own supplementary policies for vetting IT personnel. The Attorney-General's Department has sought to make all Commonwealth agencies aware of this issue and to share experience across Commonwealth vetting agencies through various forums, including the Security in Government Conference held in April 2003 in Canberra.

As each agency's use of technology differs (both between agencies and between employees within the same agency), each agency needs to consider ethical use against a particular range of factors, including those mentioned in the PSM under the heading "suitability" (extract attached as appendix A)

## Question 3 Social engineering

In broad terms the actions the Department takes to tackle social engineering as you define it include:-

- vetting in the recruitment and security assessment processes;
- deploying a range of technical applications to safeguard physical and electronic assets;
- providing education and training opportunities;
- controlling access to resources;
- monitoring uses; and
- re-evaluating needs at appropriate intervals.

The Department deploys a range of human resource management tools and strategies to keep employees up to date with developments.

The Department also issues alerts on social engineering threats to its employees, as required.

## Question 4 – Disaster Recovery

As part of the Department's overall business continuity plan, a specific disaster recover plan has been prepared addressing business critical systems as appropriate to the level of risk.

Back-up facilities are maintained at a separate site to Robert Garran Offices. Back-up tapes are held at the alternative site and by Chubb Australia. A disaster recovery kit including plans, procedures and essential configuration information is held at three sites. These documents provide for the restoration of identified critical systems on either existing (surviving) equipment or a minimal set of new or borrowed equipment. Restoration of critical systems can be achieved within 48 hours provided equipment is available.

All equipment required for interim arrangements are mass market products (PCs, and commonly used server and communications equipment). This equipment could be readily purchased locally in the case of a local fire or from interstate in the event of a Canberra-wide disaster.

## Question 5 – Archival Integrity

The Department is implementing an Electronic Records and Document Management (ERDM) System to manage the ongoing integrity of its official electronic records for record keeping and archiving.

The implementation of the system meets the official Commonwealth obligations in appropriate management and archiving of official records. Disaster recovery solutions have also been implemented in case of any emergency that affects the ERDM production systems with back-up of all ERDM data being mirrored in real-time to the back-up servers at a different physical location. Additionally, the data (records) on the ERDM production servers is backed up each night.

Supplementary Question – PSM and Inspector-General of Intelligence and Security

During the hearing, on 1 April 2003, reference was made to the Inquiry into Security Issues Report by the Inspector-General of Intelligence and Security (IGIS), Mr Blick.

Implementation of the IGIS recommendations on the Protective Security Manual (PSM) is complete. The PSM was significantly revised in 2000, cleared by the Attorney-General and endorsed by Government as the minimum, mandatory standards to apply across the Commonwealth. To ensure its policies and procedures remain relevant to the changing work environment, the Government directed the PSM be reviewed regularly. There is a particular need to address changes induced through rapid technological development. This review process is under way. Publication of a revised edition of the PSM with three updated parts should occur by December 2003.

## Question on Notice for the Attorney-General's Department – Transcript 1 Apr 03 p.136

The PSM prescribes certain mandatory standards relating to information systems security measures that must be Defence Signals Directorate (DSD) approved, authorised or certified. DSD publishes the principles it uses to approve, authorise, or certify security measures protecting information systems in the Australian Communication-Electronic Security Instruction (ACSI) 33.

Compliance with the requirements of ACSI 33 is essential if an agency is to meet mandatory security standards specified in the PSM. The subtle distinction is that Cabinet has approved the minimum standards in the PSM, whereas ACSI 33 contains guidelines issued by the agency authorised by Cabinet to advise and assist Commonwealth agencies on information system security matters.

## Question on Notice for the Attorney-General's Department – Transcript 1 Apr 03 p.140

The Commonwealth Protective Security Survey collects data from agencies to make an annual assessment of the status of protective security across all Commonwealth agencies by measuring the extent that agencies are complying with the minimum standards in the PSM. A copy of the 2002 survey questionnaire is enclosed for the Committee's information as appendix B.

The survey attempts to gauge agencies responses to computer security incidents, in the preceding 12 months, and whether they were reported via the Information Security Incident Detection, Reporting and Analysis Scheme (ISIDRAS). An agency's response to those questions is not an effective substitute for correctly reporting attempts to attack Commonwealth information systems.

I hope the above information is of assistance and please do not hesitate to contact me if the Committee requires further information.

Yours sincerely

Peter Ford
First Assistant Secretary
Information and Security Law Division

| | |
|---|---|
| Telephone: | 02 6250 5425 |
| Facsimile: | 02 6273 4180 |
| E-mail | peter.ford@ag.gov.au |