Submission No. 41

Australian Electoral Commission AEC

West Block Offices
Parkes ACT 2600

PO Box E201
Kingston ACT 2604

Telephone (02) 6271 4411
Facsimile (02) 6271 4556
www.aec.gov.au
ABN 21 133 285 851

File: 02/1726

→ Mr Luttrell.

1575

Mr James Catchpole
Secretary
Joint Committee of Public Accounts and Audit
Parliament House
CANBERRA ACT 2600

Dear Mr Catchpole

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

I refer to Mr Luttrell's letter of 29 April 2003 inviting the AEC to provide answers to additional questions that were not covered during the public hearing on 1 April 2003.

Please find attached the AEC's response to those questions.

Yours sincerely

Paul Dacey

Paul Dacey
Deputy Electoral Commissioner

12 May 2003

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

AEC response to Additional Questions

"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 AEC submission.

What action is being taken to guard against this potential problem?"

The potential risk to the privacy and security of the AEC's electronic data that is posed by social engineering has been recognised and is addressed by AEC policy. The AEC General Enrolment Manual (GEM), Security Plan and IT Security Policy (currently in draft), promote corporate strategies to mitigate the risk of a person gaining unauthorised access to information. This is achieved through various policies that together provide a form of defence in depth.

The GEM requires that written confirmation of enrolment information only be provided following a written request. The procedure is quite detailed but, in summary, signatures are confirmed against the latest Enrolment Form image before the written confirmation of enrolment is provided. Over the counter requests for confirmation may be provided verbally by an AEC officer on presentation of acceptable photographic identity.

Telephone enquiries regarding enrolment details are handled by confirming (or denying) that a person is correctly enrolled once the caller has provided detailed personal information that is likely to be only known to an individual or their family. This procedure is essential at election time when large volumes of enquires of this nature are received.

The AEC Security Plan includes policy relevant to this matter under the following headings:

Security Awareness Training

Access Control into AEC Premises

Visitors to Non-Public areas

Specific Considerations and Security Measures for Information Security

The AEC IT Security Policy includes policy relevant to this matter under the following headings:

General responsibilities of staff

Responsibilities of Supervisors of Staff

Responsibility for Systems and Data

System Manager's responsibilities

Systems Access Controls

Authorised Access to Data

Hardware and Media Security

On a more general note, the AEC's long entrenched culture of protecting the integrity and privacy of the electoral processes is additional mitigation against social engineering attacks.

"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 the AEC's disaster recovery plan?"

In terms of its electronic systems, the AEC's disaster recovery planning has to date been a part of the wider Cluster 3 Disaster Recovery Plan (DRP) which along with the AEC's Business Continuity Plan (BCP) provide a reasonably conventional disaster recovery framework. They identify systems, responsibilities, damage assessment, activation and escalation procedures, and recovery teams.

The AEC is disengaging from Cluster 3 for its desktop and server services and bringing these services in-house. The disengaged services will be covered by an AEC specific DRP being developed as part of a revised AEC BCP. The DRP will include provision of "warm-site" redundancy at a remote site. This capability is being installed as part of the transition from our outsourced vendor. The new infrastructure development has been underway since late 2002 and is planned to be fully operational by end 2003. Revised disaster recovery procedures will be arranged for services remaining with the outsource vendor (mainframe and midrange systems).

Recently, the AEC has been asked to consider whether the Electoral Roll should be considered critical in the context of the wider project to identify the Nation's entire critical infrastructure. Should the Roll fall into this category then the AEC will need to investigate whether such a classification requires heightened disaster recovery processes (moving for instance from a manually recovered operation from backup tapes held off site, which is currently the situation, to a fully redundant mainframe processing capability, a so-called "hot-site").

The Committee might wish to note that prior to every election the AEC develops additional contingency procedures that are specific to each event.