Australian Electoral Commission

SUPPLEMENTARY SUBMISSION TO THE JOINT STANDING COMMITTEE ON ELECTORAL MATTERS

COMPUTER SECURITY

Canberra

24 January 1997

1. Preamble

1.1 This supplementary submission by the Australian Electoral Commission (AEC) is presented to the Joint Standing Committee on Electoral Matters (JSCEM) in response to its "Inquiry into the 1996 Federal Election", as advertised on Saturday 22 June 1996 in all major national newspapers. The submission is supplementary to the major AEC submission, "The Conduct of the 1996 Federal Election" presented to the JSCEM on 29 July 1996.

1.2 On 13 January 1997 the Secretary of the JSCEM, on behalf of the JSCEM Chairman, wrote to the Electoral Commissioner in the following terms:

> The Chairman has asked me to write to the AEC to seek the Commission's written comments on an article which appeared in the Sunday Mail on 29 December 1996. A copy is attached.
>
> The article relates to a "Hacker" gaining unauthorised access to the AEC's computer network prior to the 1993 election. This is a matter of concern to members of the Committee, especially as it may impact on the issue of electoral integrity. The Chairman is also surprised that this matter had not been brought to the Committee's attention by the AEC.....

1.3 This submission responds to the question raised. The Sunday Mail article is attached.

2. Background

2.1 In the first week of January 1993, the AEC found that an intruder (or "hacker") had been able to gain unauthorised access to AEC computing facilities. It appears that this access was first gained through another organisation's computer. AEC officers responded with a range of counter-measures designed to minimise exposure to any further attacks, and to monitor any unauthorised activity. These counter-measures, conducted in consultation with the Defence Signals Directorate (DSD), the Australian Federal Police (AFP), Telecom, the Australian National Audit Office (ANAO), and the AEC computer suppliers, were effective.

2.3 Inquiries by the AEC, Telecom and the AFP led to a suspect being identified, seizure by the AFP of the suspect's computer, and ultimately, conviction of the suspect for a range of offences. The Director of Public Prosecutions (DPP) and the Australian Government Solicitor provided legal advice as necessary during this time.

2.4 Extensive investigations of the incidents by AEC officers acting with the assistance of the AFP, and full testing of AEC computer systems, revealed no material damage to the programs and data files maintained on AEC computers. No evidence was found of any unauthorised attempts to access the electoral roll data maintained by the AEC on the mainframe computer operated by the Department of Administrative Services. Similarly, no evidence was found of any unauthorised attempts to access the electoral roll data maintained by the AEC on the mainframe computer operated by the South Australian Government. Unauthorised access was identified as installation of trapdoors (now removed) into AEC systems, alteration of system logs to conceal the intruder's activities, and use of the AEC computer systems as a gateway into other organisations.

2.5 While the access by the intruder would have allowed entry to the AEC election and financial management systems, the AEC computer systems were used as gateways into other systems with which the AEC could be linked, rather than for any perceived benefit that might be gained from the AEC election and financial management systems or from data contained on the Commonwealth Electoral Roll. There was no indication that the intruder made any attempt to manipulate any of the AEC electoral or financial systems or data. In any event, the AEC is satisfied that the counter measures precluded any future interference.

2.6 After the 1993 federal election the AEC undertook a full review of the security of its Information Technology systems, for which an external contractor was engaged. From this review a comprehensive set of Information Technology policies, security plans and implementation procedures were developed and put in place. A continual process of review was also established and an Information Technology Security Officer was appointed to administer security policies, plans, and implementation procedures. The success of these measures will be subject to further audit during 1997.

3. Response

3.1 The AEC did not raise the eventual conviction of the offender with the 1996 JSCEM because the events leading up to his conviction did not relate to the 1996 federal election. In addition, the investigation of the matter during 1993 and 1994 by the AFP and the AEC, under tight confidentiality, precluded any reporting of the matter to the 1993 JSCEM. The AEC was advised at the time that any publicity about the investigation could make the AEC a possible target for other intruders. Further, it was clear that the 1993 federal election was not in any way affected by this security breach. Nonetheless, the then Minister for Administrative Services, and his successor after the 1993 election, were both briefed on the incident.

Mr Chris Paterson
Secretary
Joint Standing Committe on Electoral Matters
Parliament House
CANBERRA ACT 2600

Dear Mr Paterson

I have pleasure in forwarding to the Joint Standing Committee on Electoral Matters the enclosed submission from the Australian Electoral Commission:

COMPUTER SECURITY

Yours sincerely

R Bell
a/g Electoral Commissioner

24 January 1997