Mr James Catchpole
The 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 attach for your information the Australian Taxation Office's formal response to the supplementary question on social engineering forwarded by Tas Luttrell on behalf of the Committee Secretariat.

If you have any enquiries in relation to this information please contact Pam Mitchell on 02 6216 1321 or at pam.mitchell@ato.gov.au for assistance.

Yours sincerely

(original signed)
Jennie Granger
Second Commissioner of Taxation
15 May 2003

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

ATO Response to Supplementary Question On Social Engineering

Background

Social engineering is a term used to describe an intruder's manipulation of *people* (as opposed to computer systems) to obtain information that will allow unauthorised access to an otherwise secure system and/or to its associated information.

ATO Treatment

The ATO deals with social engineering threats in a number of ways as outlined in our submission. A significant component of our mitigation activities relies on the provision of mandatory user/staff awareness and education programs. These programs are part of mandatory security awareness training activities conducted by the ATO Trusted Access Branch.

They include:

- specific security training to staff on the organisation's perimeter - security guards, help desk workers etc;
- wider security training to all employees which reinforces the message that all staff have a role in protecting the ATO;
- processes to ensure training and education material is up to date and incorporated in induction programs;
- provision of instructions to employees that established procedures must be followed and if someone asks for them to be circumvented, to seek supervisor intervention; and
- reinforcement of security basics at every opportunity, eg. Logon screens, bulletin boards etc

Other areas that address the issue of social engineering include:

Policy, Procedures and Risk Assessment

ATO policies and work procedures specify a number of requirements that aid in ensuring the integrity of our information and data. These include:

- appropriate classification and disposal of corporate documents;
- defined evidence of identity protocols for use by client contact staff;
- guidelines and protocols regarding information provision;
- protection of information on desktops, laptops and personal digital assistants; and
- procedures for hosting visitors, escorting visitors and ensuring proper ID is evident.

Help desk operations

Due to their generally wide access to systems, help desk sites are an identified area of vulnerability to attacks. Mitigation measures include:

- comprehensive training of help desk operatives;
- defined scenario based procedures; and
- maintaining turnover rate of staff at a manageable level

Monitoring and Surveillance

As described in our submission, the ATO:

- uses electronic access measures for perimeter and internal access control; and
- performs security assessment tests which confirm the ATO's ability to protect its environment, its ability to detect the attack and its ability to react and repel the attack

Summary

The ATO has implemented programs which entail continuous training about security in general with an emphasis on social engineering at relevant points. We recognise the threat of people inappropriately seeking information and the many ways of trying to get that information. Coupled to that training effort, regular threat and risk analyses, physical and electronic access controls, detailed procedures, extensive forensic logging, monitoring and detection mechanisms are in place to mitigate social engineering risks.