Australian Government
Department of Education, Science and Training

OFFICE OF THE SECRETARY

Mr Bob Charles, MP
Chairman
Joint Committee of Public Accounts and Audit
The Commonwealth Parliament

Dear Mr Charles

Response to the Request for Information on Computer Related Security Breaches

Thank you for your letter of 16 September 2003 in which you requested information on the computer security related activities of the Department from July 1998. The department has undergone a number of machinery of government changes since that date:

- Department of Education, Training and Youth Affairs was established in October 1998; and
- Department of Education, Science and Training was established in November 2001.

From October 1998 to October 2002, the Department outsourced its IT infrastructure services to the Department of Employment and Workplace Relations (DEWR). Since November 2002, a number of IT infrastructure services including midrange support, desktop support and helpdesk have been transferred back to the Department. At present, the Department's Internet gateway and network infrastructure are still outsourced to DEWR. Our search is based on the records and information under the control of the Department.

In consulting with the secretariat of the Committee, it is our understanding that we are required to report on incidents that are related to activities directly under the department's control. Attached is the response to each of the queries of your letter. The contact officer to clarify any issues is Mr Tony Kwan, Chief Information Officer (02 62405983).

Yours sincerely

(signed)
Dr. Jeff Harmer

15 October 2003

Responses to Committee Inquiry

General Comments

The Department treats its security arrangements very seriously. The key points of DEST's security arrangements are as follows:

- A full time IT Security Manager.
- A detailed IT Security Policy which is approved by the Secretary and regularly updated.
- An annual review on IT security.
- IT security is part of DEST's staff induction program.
- Regular campaigns to raise security awareness.
- Regular independent website penetration tests by external consultants.
- Disaster recovery plans for DEST's key IT systems.
- Annual stocktake of IT assets.
- Regular monitoring and alerts of improper usage of IT systems.
- Regular audits on DEST's key IT systems.
- Multi-level anti-virus protection regime on DEST's IT platform. Disruption to DEST's business due to virus has been kept to a minimum.
- Strengthened password protection in DEST's systems.
- Secure coding practices training for all DEST's IT staff. Secure coding practices have been incorporated into DEST's standard system development methodology.
- Security issues reported regularly to DEST's Audit and Business Assurance Committee.

On the whole, DEST has developed and maintained a robust and reliable security regime. Despite an increased number of attempts to break into DEST's sites (which is consistent with the general industry trend), none have been successful. Any disruption to DEST's operation due to security breaches and external attacks has been kept to a minimum. There have been a number of incidents of computer thefts. The number of thefts has declined over recent years although the number of IT assets has increased. The number of laptops lost due to thefts in 1999 was 2, in 2000 was 8, in 2001 was 7, in 2002 was 6, and in 2003 was 1. DEST has approximately 170 laptops in total. The loss ratio of laptops is considered to be low by industry standard (Metagroup reported that 10-15% loss rate of laptops by private firms is not uncommon). The total number of PCs and associated equipment (e.g. CPU, hard drive) stolen in the last five years is 5 (against a total PC fleet of 2000).

The thefts of computer equipment in recent years are mainly related to home PCs and laptops in staff residence. The Department has a policy to provide home PCs to senior staff (SES and EL2) to support the requirement in accessing departmental systems outside office hours. There are at present 120 home PCs in addition to the 170 laptops which can be used for remote access (RAS) purposes. The software used for remote access is the Citrix Metaframe technology. Instead of transmitting actual data across the phone connection, only the images are displayed. No data is transmitted and stored on the RAS machines. While the loss ratio is relatively low, the Department will continue to examine options to strengthen the security arrangements of its home PCs and laptops.

We remain vigilant in addressing our security concerns. These include regular reviews, updates and improvements of our security policy and action plans. We will continue to conduct security awareness campaigns to maintain a high level of alert among DEST staff on security matters. Furthermore, DEST's IT group is in the process of developing a forward looking security architecture to address emerging security concerns.

The following addresses the questions raised specifically by the Committee:

Losses of software and/or hardware

Searches of records have indicated that over the last five years there are a total of 18 incidents involving loss or theft of equipment from DEST premises or from staff residences while they are on loan. All occurrences of the loss of equipment were reported to the Australian Federal Police for investigation.

Investigations to date with the exception of one have not resulted in the recovery of the equipment or identification of offenders. Subsequent investigations indicate that the computers reported missing did not have any sensitive information stored on them.

The following table identifies the incidents of theft of computer equipment:

Date	Nature of Incident	Comments
4/8/98	Hard drive missing from DELL PC following office move	Reported to police – not recovered
19/10/99	Two laptop PC's reported missing during office move from storeroom	Reported to police - not recovered
23/4/00	Robbery on Ground Floor and 2nd Floor 16 Mort Street between noon Sunday and 12.30pm Monday (Easter break). 8 laptops, 4 mobile phones and sundry items stolen and office damage to a total of $50,000	Reported to police - not recovered Review of Security initiated.
16/2/01	Dell Precision 620 tower PCs reported missing – stolen from 16 Mort	Reported to police – not recovered
17/5/01	New DELL GX 110 PC missing from Level 5 14 Mort Street	Reported to police – not recovered
21/5/01	DELL GX 110 PC – CPU missing from Level 1, 14 Mort street	Reported to police – not recovered
23/5/01	4 Laptop computers removed from storeroom Level 5 16 Mort Street – all Toshibas	Reported to police – not recovered
28/06/01	Toshiba Laptop stolen from residence	Reported to police – not recovered
01/9/01	Laptop stolen from residence	Reported to police – not recovered
23/11/01	Laptop computer stolen from residence	Reported to police – not recovered
?/5/02	DELL Laptop - stolen from state office	Reported to police – not recovered
20-21/5/02	DELL Latitude C600 Laptop removed from luggage	Reported to police – insurance recovery through QANTAS via Comcover
29/7/02	DELL Latitude C600 Laptop stolen from residence	Reported to police – not recovered.
23/8/02	Toshiba TECRA 8000/333 Laptop stolen from residence	Reported to police – not recovered
3/10/02	DELL Laptop stolen from residence	Recovered by Police
7/11/02	DELL RAS Laptop stolen from residence	Reported to police – not recovered
15/8/03	DELL Optiplex GX150 Laptop stolen from residence	Reported to police – not recovered
29/9/03	DELL GX 240 PC and DELL 15" LCD Panel stolen from residence	Reported to police – under investigation

Unauthorised access to computer systems

The Department's Internet gateway and network infrastructure are outsourced to the Department of Employment and Workplace Relations and therefore uses DEWR's security mechanisms to identify and respond to threats as appropriate.

The department conducts its threat and risk assessments (including its own web site penetration tests) annually and no breaches of security were detected during the reviews. None of the unauthorised attempts to access DEST's systems are successful.

Any other significant event involving information technology security

In keeping with Federal Government policy through the use of the Protective Security Manual (PSM) and Australian Communications Security Instructions 33 (ASCI-33), the Department reports breach of security to the Defence Signals Directorate using the Information Security Incident Detection Reporting and Analysis Scheme (ISIDRAS).

The following table identifies other significant incidents.

Date	Nature of Incident	Comments
5/5/00	ILOVEYOU Virus infection. Email unavailable for 8 hours	Subsequently implemented desktop virus scanning software
30/4/03	Server Crashed – A DEST web site was the target of a denial of service attack.	Incident occurred overnight – disruption to business minimal
28/8/03	Welchia virus infects a small number of corporate machines	Proactive reporting and innoculation occurring – disruption to business minimal