Submission No. 97

Australian Government
Department of Finance and Administration

Dr Ian Watt
Secretary

Our Ref: ESEC000386

Mr Bob Charles MP
Chairman
Joint Committee of Public Accounts and Audit
Parliament House
CANBERRA ACT 2600

Dear Mr Charles

Request for Information on Computer Related Security Breaches

Thank you for your letter of 16 September 2003, requesting details of any breaches of security that have occurred in the Department and it's associated portfolio agencies since July 1998. I apologise for the delay in responding.

The Department of Finance and Administration (Finance) has made significant progress in recent years to ensure that its management, integrity and security of electronic information and assets are in accordance with current legislation and practices. The Department's objectives are, and have always been, to manage information in a disciplined, consistent and secure manner.

Finance in particular has done this by:

- providing all staff with access to correct and relevant legislation, departmental policies and guidelines on its Intranet;
- regular attendance at seminars and Government information sessions dealing with changes to legislation, best practice, Defence Signals Directorate (DSD) security requirements and industry trends;
- holding regular induction courses for new employees emphasising the importance of IT security and their obligations as a Finance employee;
- introducing a requirement for all Finance employees, contractors and specific vendors' staff, to hold a current personal security clearance;
- allocation of clearly defined roles within the Department with associated responsibilities eg Chief Information Officer (CIO), Information Technology Security Advisor (ITSA) and Information Owners; and
- ongoing reviews and enhancements to policies, procedures, processes and systems.

We have developed policies in relation to Departmental Information Technology, electronic information security and asset security. These policies stipulate the correct procedures to be taken when dealing with specific types of information and the correct processes in the event of a possible theft or security breach. This policy also refers to other relevant Whole of Government information, eg *Privacy Act 1988*, the Australian

Communications Electronic Security Instruction 33 (ACSI 33), and the Commonwealth Protective Security Manual.

Attached for your Committee's consideration are responses prepared by the Department, the Australian Electoral Commission, ComSuper and the Commonwealth Grants Commission.

If you have any questions concerning any aspect of these responses, please contact Mr Dominic Staun, General Manager, Financial and e-Solutions Group on 6215 3518 regarding the Department and Mr Sean Giddings, Parliamentary and Corporate Support on 6215 3590 for the Portfolio Agencies.

Yours sincerely

I J Watt
7 November 2003

Losses of Software and/or Hardware

Since July 1998, Finance has lost four (4) laptops; two were destroyed in the January bushfires in Canberra and two were stolen, although one has since been recovered. The users have reported that there was no confidential data on these laptops. In addition, one departmental laptop from a Ministerial office was also stolen. In accordance with internal Finance policies and guidelines, all occurrences of stolen equipment have been reported to the Australian Federal Police. All stolen equipment was reported to police and were subject to investigation. All police investigations have been concluded and no legal action has been taken. Staff responsible for the stolen items have been counselled. The Department's intranet site draws to the attention of all departmental officers who are issued with Commonwealth assets the need to observe the guidelines governing the safe keeping of assets.

There has been no reported loss of software within Finance. The Department's IT services provider (IBMGSA) is responsible for the management of the majority of software utilised within the Finance IT environment. Additionally, the Department, from time to time, provides software to Finance staff, contractors and external service providers for the purpose of conducting Finance's business. To support this requirement an internal policy was developed for these users to provide guidance on the use of software in the Finance IT environment.

Unauthorised Access to Computer Systems

The Finance network is a controlled environment, with all network devices configured with security mechanisms that only allow access by authorised personnel. Finance IT policies stipulate the requirements of user passwords and offer a guide to creating and maintaining strong passwords. Additionally the Department's corporate firewall and gateway is Defence Signals Directorate (DSD) accredited and includes intruder detection systems with 24 hour monitoring and response.

Over the requested reporting period there has been no recorded incidents of unauthorised access to the Finance network.

A major component of Finance IT is the Internet websites. These sites are hosted on servers outside the Finance network in physically secure areas. The data held on these servers has no classification and is for public consumption. The Internet servers are configured with intruder detection systems with 24 hour monitoring and response. During the requested reporting period, Finance has recorded five (5) unauthorised access attempts via the Internet by unknown persons.

On all occasions the incidents were reported to DSD via the Information Security Incident Detection, Reporting and Analysis Scheme (ISIDRAS). Internal investigations by the Department's IT security team and IBMGSA were completed for all the incidents with additional assistance being requested by DSD for two (2) of the incidents that required further investigation. As a result of the investigations, the Department is confident that no loss of data or unauthorised access occurred.

Any Other Significant Event Involving Information Technology Security

A significant breach of IT security in the reporting period related to the misuse of a password by a contractor who transferred substantial funds to a private company without authorisation. The contractor was charged with fraud, tried in the ACT Supreme Court, convicted, and sentenced to a 7 ½ year gaol term. Finance is continuing with its civil litigation against a number of defendants to recover the monies defrauded.

Finance Response to Shergold Inquiry about Submissions to the Committee

- Finance does not intend making a formal submission to the JCPAA in relation to this matter. If for unforseen reasons, circumstances change, we will immediately notify Dr Peter Shergold.
- Interestingly though, the JCPAA website lists answers to Questions on Notice as "Submissions". Finance provided on 14 July 2003 the Committee with answers to questions taken on notice during its appearance before the Committee on 2 June 2003. A copy of this "Submission" can be found at http://www.aph.gov.au/house/committee/jpaa/electronic_info/submissions/sub65.pdf.
- For Dr Shergold's information, officers of the Department have appeared as witnesses before the Committee on 2 June 2003 and 8 October 2003. In relation to the 8 October appearance, Committee members directly queried Finance witnesses on the security of IT equipment in Electorate Offices.

Australian Electoral Commission (AEC) response to JCPAA Questions on Computer Related Security Breaches

Losses of Software and/or Hardware

Since July 1998, the AEC has had 15 PCs, 2 laptops and 16 monitors stolen.
Each of the machines had the AEC's standard image (Windows and MS Office), Lotus Notes and in-house applications software. No other software was stolen. Each theft was reported to the police. Only one of the stolen hard disk drives has ever been recovered and prosecution proceeded through the Courts. Criminal proceedings have not commenced in any of the other cases. No investigations have linked thefts to staff members of the AEC.

Unauthorised Access to Computer Systems

The AEC has three levels of firewall protection against unauthorised access from external sources. The AEC is part of Cluster 3 and uses the services of an outsource service provider operating a DSD approved firewall. The AEC has not been involved in any following up of incidents of unauthorised access. The AEC's policy and procedures on IT Security clearly set out rules for authorised access and no major incidents have been detected.

Any Other Significant Event Involving Information Technology Security

Nil

ComSuper response to JCPAA Questions on Computer Related Security Breaches

Losses of Software and/or Hardware

In the 1999 annual stock take one digital 200MMX(ComSuper asset 702094) could not be located. A Toshiba Laptop and bag (model 320 CDS) was stolen from an employee's residence during a break-in on December 10, 1999. This was reported to the AFP and a Statutory Declaration signed by the employee. No information on the laptop was classified for security or other purposes. In the 2000 annual stock take one digital 15" monitor (ComSuper asset 701727) could not be located.

Unauthorised Access to Computer Systems

There have been no incidents detected.

Any Other Significant Event Involving Information Technology Security

ComSuper has had no significant IT security incidents other than the "I Love You" virus which caused two hours downtime while the network was verified clean.

Commonwealth Grants Commission response to JCPAA Questions on Computer Related Security Breaches

Losses of Software and/or Hardware

Since 1998 3 laptops and 1 projector have been stolen, no other software was stolen. The thefts were reported to the police and criminal proceedings have not commenced, no investigation has linked the theft to a staff member of the Commission.

Unauthorised Access to Computer Systems

A hacker accessed the Commonwealth Grants Commission (CGC) web site in February 2000. The incident involved a nuisance attack on the CGC web page where a message was left. The message was in Portuguese and looked to have originated from Brazil. An investigation revealed that our ISP at the time (Dynamite) had not applied password security to our site. This was rectified and we have had no other incidents of this type.

As mentioned, this was a nuisance attack. Our web site contains public information only and is not connected to our LANs. We have since changed ISP (now Netspeed) and have increased security by installing our own firewall. We are also in the process of gaining a security certification from Defence Signals Directorate for our new firewall.

Any Other Significant Event Involving Information Technology Security

Nil