Submission No. 75

Australian Government
Attorney-General's Department
Secretary

17 October 2003

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

I refer to your letter of 16 September 2003 requesting details of any breaches of computer security that have occurred in the Attorney-General's Portfolio since July 1998.

I enclose the Portfolio's response which is submitted in accordance with the deadline extension granted by the Committee Secretary.

The action officer for this matter is Barry Jeffress who can be contacted on (02) 6250 6162.

Yours sincerely

RJCornall

Robert Cornall
Secretary

ATTORNEY-GENERAL'S PORTFOLIO
INFORMATION ON COMPUTER RELATED SECURITY BREACHES
FOR THE JOINT COMMITTEE OF PUBLIC ACCOUNTS AND AUDIT

Attorney-General's Department

1. In 1999 three new desktop PCs which did not contain any Government information were removed from the Department's computer training centre. The incident was reported to the police. No items were recovered nor were charges laid.

2. In 2000 a laptop computer was left by a member of the Attorney-General's staff in a taxi in Perth. It is not clear from the Department's records if there was any classified Government information. The incident was reported to the police and the item recovered from the taxi driver's home. No charges were laid.

3. In 2001 a desktop PC is believed to have been erroneously removed by cleaners from the Department's Help Desk area in the misunderstanding it had been discarded. The incident was investigated by the police, but no charges were laid. The item was not recovered.

4. In 2003 a laptop computer and floppy disk were stolen from a motel room in Tasmania. The laptop was protected by encryption and contained information to protected level. There is an high degree of confidence the information on the laptop could not be accessed. The floppy disk was not protected by encryption. The police investigated, but no charges were laid or the items recovered.

5. The laptop computers and desktop PCs all contained the standard operating environment which included the operating system, virus protection and office automation software. The desktop PC also contained the Department's development suite of File Maker Pro and Visual Basic.

6. A Personal Digital Assistant (PDA), which did not contain classified Government information, was reported lost in Canberra. The incident was reported to the police, however the item was not recovered.

7. There are no known instances of unauthorised access to computer systems or any other significant events involving information technology security.

The following contributions have been provided by the Attorney-General's Portfolio Agencies.

Administrative Appeals Tribunal

1. In November 1998 the Assistant Registrar's laptop computer was stolen overnight from the Sydney office. The incident was reported to the police, however the item was not recovered or any person apprehended.

2. In August 1999 the President's laptop computer was stolen overnight from the Sydney office. The incident was reported to the police, however the item was not recovered or any person apprehended.

3. In September 1999 the Assistant Registrar's laptop computer was stolen overnight from the Sydney office. The incident was reported to the police, however the item was not recovered or any person apprehended.

4. In October 1999 a 32 MB RAM memory card was stolen. There is no record on file of the incident being reported to police. The item was not recovered.

5. In April 2003 the President's laptop computer was stolen in transit while in the custody of TNT Couriers. There is no record of recovery or reporting of the incident to the police.

6. There are no known instances of unauthorised access to computer systems or any other significant events involving information technology security.

Australian Crime Commission (ACC) *– Formerly the National Crime Authority (NCA) and Australian Bureau of Criminal Intelligence (ABCI)*

1. In October 2000 an ABCI laptop computer was stolen from a staff member's home in Canberra. The computer was encrypted and password protected and contained no operational or intelligence information. The theft was reported to the police, however no persons have been apprehended or the item recovered.

2. In April 2001 an NCA laptop computer was stolen from an NCA vehicle in Sydney. The computer was encrypted and password protected and contained NCA software and material. There has been no indication that NCA material has been compromised. The theft was reported to the police, however no persons have been apprehended or the item recovered.

3. In June 2001 an NCA laptop computer was stolen from a staff member's home in Melbourne. The laptop was encrypted and password protected, and contained no NCA material. The theft was reported to the police, however no persons have been apprehended or the item recovered.

4. In June 2002 an NCA laptop computer, was stolen from a staff member's home in Brisbane. The computer was encrypted and password protected and contained no NCA material. The theft was reported to the police, however no persons have been apprehended or the item recovered.

5. In January 2003 the personal laptop computer of an ACC staff member on duty in Melbourne was stolen from his vehicle. The laptop contained ACC software and material, and a mixture of encryption and password protection. There has been no indication that ACC material has been compromised. The theft was reported to police, however no persons have been apprehended or the ACC software and material recovered. The staff member was counselled on the use of unauthorised equipment, and the procedures in relation to the use of unauthorised equipment were reinforced with the staff of the relevant ACC unit.

6. In July 2000 an NCA laptop computer containing NCA material was used externally to connect to the Internet. The laptop was not encrypted and no material was exposed to possible compromise. An internal investigation was conducted and concluded that NCA procedures had not been followed. The officer was counselled.

7. In August 2002 an NCA IT Administrator password was provided to an NCA officer, without authority, via an insecure medium. The incident was reported immediately. The risk to the NCA system at the time was not judged to be significant. The officer was counselled and the Administrator passwords on all relevant NCA PCs and laptop computers were changed.

8. In May 2003 the Western Australia Police Crime Stoppers received an anonymous e-mail offering confidential information. The correspondent would only deal with an ACC member. E-mail contact was made which generated an e-mail response containing a virus. The virus did not infect the ACC system, however the ACC considered it was the subject of an electronic sabotage attempt. Efforts to trace the identity of the e-mail correspondent were unsuccessful. The message originated from the USA but no additional identifying particulars could be obtained. No further e-mails have been received from this correspondent.

9. In July 2003 a user identification and a password were provided by an authorised user to an unauthorised user. The unauthorised user was quickly detected and ongoing access to the ACC system was refused. The authorised user was formally reprimanded by a letter of censure. A high priority instruction was issued to all users of that system reminding them of the appropriate security standards to be followed in such matters.

10. The ACC is part of a secure gateway environment built and managed by a private company to service a number of Commonwealth law enforcement agencies. It is certified by the Defence Signals Directorate (DSD). The gateway incorporates several categories of security control, including firewalls, intrusion detection systems and anti-virus software. The ACC network and its Internet host site have not experienced any successful virus or hacker attacks at the client level since joining the gateway. The ACC LAN has procedural and access security controls to limit and govern access on a need-to-know basis.

Australian Customs Service

1. In July 1999 a laptop computer and Lite Pro were stolen from Allara House. The items were last sighted at 11am on the day of the incident and noticed missing at 6.45 pm that evening when the reporting officer went to lock them away. The laptop was password protected and contained no information above In-Confidence. The incident was reported to Internal Affairs, however the items were not recovered.

2. In September 1999 an Electronic Data Systems (EDS) issued laptop computer, and personal items were stolen from a private residence. The laptop was password protected and contained no sensitive information. The incident was reported to and attended by the police, however the items were not recovered.

3. In November 1999 an EDS issued laptop computer and fax/phone, and personal items were stolen from a private residence. The laptop was password protected and contained no

sensitive information. The incident was reported to and attended by the police, however the items were not recovered.

4. In July 2000, an Internet modem was discovered missing by staff at 40 Allara Street. The modem had no data implications. The incident was reported to Internal Affairs, however the item was not recovered.

5. In September 2002 a laptop computer was accidentally left at a hotel in Canberra. The incident was reported to IT Security. The laptop was password protected and contained no information above In-Confidence. Most of the information was presentations and schedules. The laptop was not recovered.

6. In January 2003 two EDS desktop PCs were reported as missing from Link Road, Mascot. The incident was not reported to the police by Customs as the computers are EDS property, did not contain Customs information and were never used by a Custom's employee. The items have not been recovered.

7. In April 2003 a briefcase containing a keyed randata encryption modem was lost. The briefcase was placed on a Qantas aircraft as cargo at Broome but could not be found on arrival at Darwin. The incident was investigated by IT Security, however neither the briefcase or modem were recovered. The encryption codes were changed to remove any risk of the modems being used to access Customs networks.

8. In June 2003 two line encryptors that Customs loaned to the Department of Immigration, Multicultural and Indigenous Affairs (DIMIA) were lost. The encryptors were left in the computer room in a building vacated by DIMIA. The contractor demolishing the building advised that the contents of the computer room were removed and taken to Pialligo landfill where it was dumped and buried along with other materials from the demolished buildings. The incident was reported by EDS to the Technical Infrastructure Section who followed it up with DIMIA. DIMIA advised that the encryptors had been accidentally disposed of. No further action was taken as the risk of compromise to Customs IT networks was assessed as negligible.

9. In August 2003 two IT servers were allegedly stolen from Customs premises at Sydney airport. The police investigated and two persons have been charged with the theft. The matter is currently before the court. The servers have been recovered. Customs have also been advised that in the record of interview one of the accused has alleged that two other items of computer equipment were also stolen. The theft of this equipment has not been verified.

10. In August 2003 a laptop computer, which did not contain any Customs data, was stolen from Customs House at Darwin. The police investigated, however the item was not recovered or any person identified.

11. In October 2003 a caged storage area for obsolete equipment at Allara House was broken into and three unserviceable laptop computers stolen. These laptops had been prepared for disposal and did not contain hard drives or Customs information. The police were notified.

12. In August 1998 a Customs Officer who had authorised access to the AFP Intell II database gave his user ID and password to another Customs Officer to allow that person to access

the database for work related purposes. The incident was reported to the police and Internal Affairs. The two individuals were counselled.

13. In August 2000 an unsuccessful attempt was made to access the Customs network via the 'annex box'. Security on the computer system effectively prevented unauthorised access to Customs networks. The AFP investigated and subsequently identified two male persons in Adelaide, however there was insufficient evidence to lay charges. AFP also believe they attempted to gain access to Customs dial up telephone lines. The major impact was the loss of remote dial-up access and defacement of the logon message. No data was compromised.

14. A number of virus attacks have occurred. The most significant was the 'GONER' virus. The major impact was a three hour loss of e-mail services. EDS investigated the incidents. The attacks were considered to be random external attacks and accidental internal attacks. No data was compromised.

Australian Federal Police (AFP)

1. During the reporting period the AFP had 13 laptop computers stolen and the Australian Protective Service (APS - which became an operating division of the AFP on 1 July 2002) one. All laptops included proprietary software such as Microsoft Office and is not specifically listed unless software was lost or stolen. All reports of theft or loss of IT equipment are investigated by AFP Professional Standards and APS Security Integrity Section to determine the threat and risk to AFP/APS operations of the loss of data held on laptops or hard drives. All AFP laptops use DSD approved encryption software "PC Vault" and do not hold any material above Highly Protected. None of the AFP laptops stolen were in use by staff involved in national security activities and were stolen from private residences or vehicles. None of the thefts of the laptops were assessed as having been specifically targeted at obtaining police computers or as having significant impact on AFP or APS operations in relation to the data contained on the hard drives. APS laptops did not previously have any additional security software installed, but are now required to have the AFP standard encryption software installed. The stolen APS laptop was in use by the National Training Centre and contained training material.

2. The AFP also had a laptop computer hard drive and a memory stick stolen during the period. The theft of the hard drive occurred when a laptop was being repaired to correct a fault where the data on the drive was found to be corrupted. Investigations indicated that this was an opportunistic theft and that no AFP information was compromised. Also during the reporting period the AFP reported three dial in modems as being lost or stolen. These modems allow members to dial-in and access the AFP system from remote locations and are password protected. All modems were deactivated immediately upon report and subsequent investigations did not indicate any compromise of AFP data or systems.

3. Only one AFP laptop computer was recovered in the reporting period.

4. Unauthorised access to AFP/APS computer systems has been separated into two groups, internal, which includes staff misusing passwords or accessing information which was outside the scope of their duties or in breach of guidelines (ie browsing) and external which includes attempts to gain access or attacks upon computers or systems by non employees.

5. In the reporting period the AFP had four reported external unauthorised attempts to gain access to an AFP computer. Two of these reports relate to laptops, which were not connected to the AFP computer system. Access was not gained due to the security software in place, nor was any person identified as responsible for the attempts. The remaining two incidents relate to attempts to gain access to the AFP system from an external source point. These attempts were unsuccessful. Investigations did not identify the persons responsible.

6. The AFP had six reported internal unauthorised accesses all relating to misuse of logon codes. In these reported instances no operational material was accessed with subsequent investigations revealing that messages had been sent on the AFP internal email system. Members were counselled and reminded of their responsibilities for securing AFP computers under the AFP Guidelines.

7. Within the APS, there were two reports of internal unauthorised accesses involving standalone computers where unauthorised software and data was attempted to be installed. Two other reports relate to inappropriate use of the APS computer system. No persons have been identified as responsible for these matters.

8. In the reporting period the AFP had 17 virus attacks and four incidents of attempted spamming, while the APS had no reported incidents. The AFP has a robust system of firewalls and antivirus software which prevents unauthorised access and restricts certain material from being transmitted on the AFP network. None of the reported incidents was successful in causing any detriment to the AFP system. Investigations into the virus attacks indicated that they were accidentally introduced via emails or access to the internet. The spamming attacks were of a low order of sophistication and do not appear to be deliberately targeted towards the AFP. Investigations indicate that the AFP was an incidental recipient of the attacks.

9. Further to the above, and as a consequence of the reported theft of Australian Customs Service computer servers, the AFP undertook precautionary countermeasures by securing access to the AFP system by Customs staff. Investigations indicate that there was no compromise of AFP data or systems in this incident.

Australian Institute of Criminology

1. In July 2003 the following items were stolen due to burglary:

   - 3 desktop PCs
   - 3 barcode scanners
   - 3 analogue handsets
   - 1 smart label printer
   - 1 image scanner
   - 1 data projector
   - 3 OEM versions of Windows 2000 workstation
   - 3 copies of Office 2000, and
   - 3 copies of First 22 Library Catalogue tool.

2. All users store all data on the network, therefore there was no actual data loss. The burglary was reported with the police attending the site. The results of the investigation are pending. No equipment has been recovered at this stage.

3. In September 2003 the web server was hacked but due to procedures and methodology in place, the effects and damage were minimal. The latest intrusion detection system has been installed and is operational.

Australian Security Intelligence Organisation

1. During 2000 a single laptop computer which contained no classified material was stolen, along with other belongings, from an officer's private residence. The police investigated the theft, however it was never resolved or the laptop recovered.

2. There was no unauthorised access to computer systems or any other significant events involving information technology security.

CrimTrac

1. A portable laptop computer issued to an agency official was stolen from his locked car at an inner Sydney parking station on 13 May 2002. The theft was immediately reported to the police and was investigated internally. The computer was recovered some weeks later, having been purchased over the Internet by an unsuspecting buyer. The computer's hard disk had been wiped clean, but it had contained only standard PC applications and no sensitive information. No arrests have been made over this theft and the laptop is now being used in the agency.

2. A recent stocktake failed to locate some IT-related items, which, according to accounting conventions have been declared 'written off' until their status can be determined. It is most likely these items have been distributed to one of thirty nine locations supported by CrimTrac throughout Australia's police jurisdictions. Among these items are seven desktop monitors, six scanners and other IT-related items on which data cannot be stored, hence information security has not been compromised. There is no indication that these items were stolen and it is probable they will be located and be re-absorbed into the assets register in the current financial year.

3. There has been no unauthorized access to computer systems, or significant events involving information technology security.

Director of Public Prosecutions (DPP)

1. Two separate break-ins within a short period of time in 2001 resulted in the theft of 11 desktop PCs from the library at Head Office. Increased physical security measures were introduced and there have been no further incidents.

2. Two laptop computers were stolen from regional offices at Hobart and Melbourne in 2002 and 2003 respectively, and another was lost, presumed stolen in 1999. It is understood that

they did not contain any sensitive information, however the information may not have been in the public domain.

3. The DPP has a standard operating setup for its laptop computers and desktop PCs. The software on all devices are 99% the same. The software on the PCs should not store data as the policy requires that data be stored on the network. Laptops have an encrypted directory for the storage of any work data. The standard software is as follows:

   - Window 2000 Professional
   - Microsoft Office
   - Office Macro programs
   - FIRST Library system client
   - Corporate systems CARS, CRIMS etc
   - Winzip
   - Citrix clients
   - eTrust Inoculate IT
   - SAPR3 client, and
   - Acrobat Reader.

4. With the exception of the laptop computers, the incidents were reported to the police for investigation, however no items were recovered or any person prosecuted.

5. There are no known instances of unauthorised access to computer systems or any other significant events involving information technology security.

Family Court

1. In November 2000 a notebook computer with no classified information and containing a standard operating system and office automation products was stolen from the Newcastle Registry. The incident was reported to the police, however the item was not recovered or any offender identified.

2. In November 2001 a notebook computer with no classified information and containing a standard operating system and office automation products was stolen from the Adelaide Registry. An internal investigation was conducted, however the item was not recovered or any offender identified.

3. In February 2002 a notebook computer awaiting build and deployment, and containing no software, was stolen from the Canberra Registry. The incident was reported to the police, however the item was not recovered or any offender identified.

4. In March 2003 a notebook computer with no security classified information and containing a standard operating system and Microsoft Office products was stolen from the Dubbo Registry. The incident was reported to the police, however the item was not recovered or any offender identified.

5. No incidents have been identified other than virus infections. On these occasions the security of the Family Court's information technology environment was not compromised.

6. The Family Court is continuing to maintain and improve its information technology security environment. Currently, this includes a review of the Court's Information Technology Security policy, the continued improvement of our environment in alignment with the Commonwealth's Protective Security Manual, the implementation of an even more secure gateway environment, and the hard disk encryption of a significant quantity of the Court's notebook environment.

Federal Court

1. During the last five years there have been five instances of computer loss comprising two laptop computers, two desktop PCs and a file server. Three instances were theft from residential premises where equipment was used for official purposes, and the others were lost in transit with the courier company meeting their replacement costs. The computers had standard Court software consisting of Windows and Microsoft Office. The server was loaded with the base Novell Netware only, ready for migration/implementation at the destination site. The police investigated the residential thefts. No items were recovered or offenders apprehended.

2. There are no known instances of unauthorised access to computer systems or any other significant events involving information technology security.

Federal Magistrates Service

1. On 25 November 2001 one notebook computer was lost. The notebook was left in the back of a taxi in which a staff member had been travelling. It is understood that no sensitive information was contained on the computer, with access to the computer requiring a 'power on' password. The incident was reported to the police, however the notebook was not recovered.

High Court of Australia

1. In early 2000 a laptop computer was stolen by a taxi driver in Melbourne. The incident was reported to the police and investigated. The item was not recovered nor the perpetrator identified.

2. There are no known instances of unauthorised access to computer systems or any other significant events involving information technology security.

Human Rights and Equal Opportunity Commission

1. In 1998 three desktop PCs and one laptop computer with no security classified information were lost, presumed stolen, from the Commission's premises in Sydney. The losses were reported to the police and investigated. The items were not recovered.

2. In 1999 one laptop computer with no security classified information was lost, presumed stolen, from the Commission's premises in Sydney. The losses were reported to the police and investigated. The item was not recovered.

3. In 2001 three desktop PCs, one laptop computer and one handheld notebook with no security classified information were lost, presumed stolen, from the Commission's premises in Sydney. The losses were reported to the police and investigated. The item was not recovered.

4. There has been no unauthorised access to the computer systems during the reporting period or any other significant events involving information technology security.

Insolvency and Trustee Service, Australia (ITSA)

1. In January 2001 two new and unused laptop computers without any corporate or personal information were alleged to have been delivered to ITSA's national office, but were not received. The supplier replaced the laptops at no cost, but did not admit liability. It was recognised that there had been a failing with delivery. The incident was reported to the police and investigated, however no items were recovered and no legal action taken.

2. During May 2002 two new and unused desktop PCs were reported missing from the basement storeroom of the building in which the Melbourne office operates. The incident was reported to the police and investigated, however no items were recovered and no legal action taken.

3. There are no known instances of unauthorised access to computer systems or any other significant events involving information technology security.

National Native Title Tribunal

1. In December 2000 one Tribunal supplied laptop computer was stolen from a member's residence along with a privately owned personal computer and a number of other items. The equipment contained administrative and non-confidential information only. The police attended, however the items were not recovered and no arrests were made.

2. In May 2001 four Tribunal laptop computers containing administrative and non-confidential information only were stolen from the Melbourne Registry. The police attended, however the items were not recovered and no arrests were made. Provision has been made to securely attach laptops to desks.

3. In December 2002 there was a minor defacement of the Tribunal's new 'test' website during the testing phase of development. There was no impact on the Tribunal and Defence Signals Directorate was not advised. The Tribunal's outsourcing partner was requested to examine it and reinforce (harden) the security of the Tribunal's web server prior to going 'live' to avoid future attempts at breaching security.

4. The Tribunal's production website was defaced by an organisation whose sole aim was to highlight the vulnerability of various Microsoft products. The web site was fully restored within twelve hours of the original defacement. As it was considered to be a Category 3 incident Defence Signals Directorate was advised. Access was gained because the web server had not been "hardened" as requested, and versions of software were out of date. Since the Tribunal has taken over full responsibility of the environment, security of all servers has been increased significantly (with the help of Defence Signals Directorate) and

processes are in place to ensure the latest versions of software and patches are loaded as they become available.

Office of Film and Literature Classification

1. In 1999 two laptop computers with the standard Microsoft Office suite software and no sensitive data were stolen. One laptop was stolen from the Director's vehicle and the other from a Client Liaison Officer. The incident was reported to the police, however no items were recovered.

2. There are no known instances of unauthorised access to computer systems or any other significant events involving information technology security.

Office of Parliamentary Counsel

1. Since July 1998 there have been two computer related security breaches. In each case a single memory chip was removed from a computer that was not turned on and had not been used for several weeks. The chip was random access memory only which stores data only while the computer is turned on, and therefore the risk of any information being retrieved from these chips is extremely low. There was no evidence that access had been gained to the computers' hard disks.

2. The investigations into the incidents did not reveal any additional information, including the identity of the offender or the location of the chips.

Other Portfolio Agencies

1. All other agencies within the Attorney-General's Portfolio provided advice that no breaches had occurred.