DEPARTMENT OF IMMIGRATION AND MULTICULTURAL AND INDIGENOUS AFFAIRS

Secretary

File Ref: ADF2000/3706

Joint Committee of Public Accounts and Audit
Parliament House
Canberra ACT 2600

Attention: Bob Charles, MP
Chairman

Dear Mr Chairman

Request for Information on Computer Related Security Breaches

I refer to the Committee's request as per above, dated 16 September 2003, and provide this response for the portfolio. The information provided for the department was compiled from incident reports lodged with the DIMIA Security Section and from follow-up telephone calls to the relevant areas. Your questions were passed to other portfolio agencies and service providers. Their responses are incorporated in this reply. The department does not have access to the records of the other agencies and service providers.

Responses were received from:

- 90East Pty Limited,
- Aboriginal Hostels Limited,
- Aboriginal and Torres Strait Islander Commission,
- Aboriginal and Torres Strait Islander Services,
- Anindilyakwa Land Council,
- Australian Institute of Aboriginal and Torres Strait Islander Studies,
- Carlson-Wagonlit,
- Central Land Council,
- ClientWise Pty Limited,
- Computer Sciences Corporation Limited,
- Department of Immigration and Multicultural and Indigenous Affairs,
- Indigenous Business Australia,
- Indigenous Land Corporation,
- Insightech (Converga - part of Outsource Australia),

DIMIA

Benjamin Offices, Chan Street Belconnen ACT 2617
PO Box 25 Belconnen ACT 2616 • Telephone (02) 6264 2560 • Facsimile (02) 6264 2670

Notes on the events:

i) A total of 19 cases of unauthorised access by DIMIA staff were reported by the Values and Conduct Section from July 1998 until present and these included:

- 10 alleged cases of unlawful access to DIMIA databases;
- 8 cases where people have allegedly accessed DIMIA databases without the authority to do so; and
- 1 case of a staff member inappropriately using a logon ID.

These incidents were detected by regular checks of audit and access logs.

The above cases were investigated mostly under the Public Service Act with a small number investigated criminally.

The majority of the cases investigated were found to be unsubstantiated. The cases that were found to be substantiated had sanctions imposed ranging from a reprimand, reassignment in duties, or deduction in salary to termination of employment being the most serious. In one case the employee had their employment terminated and subsequently was charged and convicted of a criminal offence.

ii) An account was created by a staff member of CSC and used to download inappropriate material from the Internet. Investigations as to who was responsible for this were inconclusive. There is no evidence of data compromise.

iii) On two occasions, default access to the mail database was changed accidentally. Access rights were restored to the default "No Access". There is no evidence of data compromise.

iv) Unauthorised changes were made to the Indigenous Land Corporation's (ILC) web site in 2000. ILC state that there was no evidence that the unauthorised access went beyond the Internet server during this incident.

iii) Encryptors were left in the decommissioned computer room of the Benjamin Offices, prior to the building being demolished. The devices could only be used with a matching pair, were for backup use and had not been connected to the network.

iv) The antivirus strategy that has been implemented by CSC ensured that the infections were contained with minimal impact to users. CSC reported these incidents via the ISIDRAS[2] scheme to the Defence Signals Directorate.

v) As a result of DFAT removing their connection to a secure network, which is also utilised by DIMIA, internet addressed email (firstname.lastname @dfat.gov.au) between the two agencies was transmitted via the Internet. A secure method for sending email between DIMIA and DFAT, whether it is addressed using Lotus Notes or Internet addresses, was implemented.

vi) Improper tape transport - CSC utilised Australia Post instead of "safe hand" delivery. All CSC lines of service have been instructed to use TNT FailSafe only. CSC has implemented new procedures for off-site storage of tapes. The tapes were returned to DIMIA and no tampering of the tape cases was evident.

vii) An IP address is the Internet address of a computing device. There have been two reported incidents of IP addresses being transmitted using an unencrypted email message. Staff members were instructed that such information is not to be sent via the Internet. There is no evidence of compromise or impact.

viii) There have been several reported incidents of IP addresses sent over unencrypted facsimile lines. Staff members were instructed that such information is not to be faxed. There is no evidence of compromise or impact.

ix) CSC inadvertently removed access controls from data during a file server reorganisation. The possible impact was in terms of confidentiality – ie access to the data was available to unauthorised DIMIA staff. The incorrect settings were identified by DIMIA Security staff and rectified within 24 hours. CSC procedures were reviewed and checklists implemented. Security awareness refresher training was provided to staff members.

x) Virus infection - three workstations at the Indigenous Land Corporation were infected by the "Love Bug" virus. Signature files were updated and applied.

---

[2] Information Security Incident Detection, Reporting and Analysis Scheme - established by DSD to collect information on security incidents which affect the security or functionality of Australian Commonwealth Government computer and communication systems.

Luttrell, Tas (REPS)

From: Committee, JCPAA (REPS)
Sent: Thursday, 13 November 2003 2:32 PM
To: Luttrell, Tas (REPS)
Subject: FW: response to JCPAA questions re computer related security breaches

Letter of Reply 171003.doc (14...

Tas, could you let Sheridan know if this is a sub???

Thank you
Maria

-----Original Message-----
From: michele.foster@immi.gov.au [mailto:michele.foster@immi.gov.au]
Sent: Thursday, 13 November 2003 3:04 PM
To: Committee, JCPAA (REPS)
Subject: response to JCPAA questions re computer related security breaches

Tas,
As discussed here is the email version ahead of the hard copy. You will note that the signature date on this version, which the Secretary and the Minister have cleared is October 2003. When the hard copy comes back from the Minister's office I will get the Secretary's signature and send to you.

Grateful for a reply email so that I know that you received this.

Michele Foster
ph) 6264 1429; 0413 458 371

(See attached file: Letter of Reply 171003.doc)