Now UNCLASSIFIED as Submission No. 90.

IN-CONFIDENCE

Submission No. 100

Australian Government
Australian Customs Service

Customs House
5 Constitution Avenue
Canberra ACT 2601

hr 15/9

The Secretary
Joint Committee of Public Accounts and Audit
Parliament House
CANBERRA ACT 2600

Dear Mr Catchpole

Please find enclosed a supplementary In-Confidence submission from the Australian Customs Service in response to the Committee's request for further information on the theft of computer equipment from Customs premises in Sydney. This matter was the subject of evidence provided to the Committee at its hearing on 5 September 2003.

I would ask that the submission be kept In-Confidence and not publicly released as it contains information concerning Customs protective security environment and procedures.

Yours sincerely

Gail Batman
National Director
Border Intelligence & Passengers

12 September 2003

IN-CONFIDENCE

Australian Government
Australian Customs Service

Supplementary Submission to the Joint Committee on Public Accounts and Audit

Report on theft of two servers from Customs Office, Sydney 27 August 2003

IN-CONFIDENCE

Introduction

1. As at 12 September, there are ongoing investigations into this incident by the Australian Federal Police, the Defence Signals Directorate and the independent external review group appointed by the Minister for Justice and Customs.
2. The referral to the Defence Signals Directorate was made in accordance with their role in information security, as set out in Section 7c of the Intelligence Services Act 2001.
3. These investigations may have information about this incident which is not available at this time to Customs.
4. Further, as these investigations progress more information may come to light.
5. The report is based on the best information available to Customs as at 12 September.

The Incident

6. At 16:00 hours on 27 August 2003 an electronic access card for the computer network server room at Level 3, Charles Ulm Building. Link Road, Mascot was signed out to an individual believed at the time to be a contracted technician
7. A Customs officer at Link Road later reported network problems to the EDS field services officer (FSO) who advised him to reboot the server. The Officer noted the access card was not in its normal place and requested the attendance of the EDS FSO, who arrived at approximately 19:40 hours. He discovered that there were two computer servers missing from the room.
8. The two missing servers are Compaq ML370 G2 servers. One is an exchange server (electronic mail server) and the other a backup domain controller. No business data resided on these servers. The exchange server contained the Customs global address book listing staff names, user IDs, email addresses and mailbox names. Email messages and attachments are stored on a separate device in the same room which was not removed.
9. The backup domain controller contained an encrypted list of Customs network user IDs and passwords, server names and network IP addresses. An external attack, or intrusion, into Customs network using these lists is not possible due to firewall protocols.

Immediate Response

10. Customs Security and then NSW Police were advised immediately the theft was discovered.
11. In conjunction with the NSW police investigation Customs convened a crisis response team on 28 August 2003. This team reviewed the matter to develop worst-case scenario and

treatments, which included eliminating particular dial-up access to the network and a managed change of all passwords by Customs staff and other authorised users of the Customs network.

12. The crisis response team then contacted relevant Australian Government information technology investigators in the Australian Federal Police and the Department of Defence on 29 August 2003.
13. The AFP now has charge of the investigation.
14. The nature of the ongoing investigation is sensitive, however to date there is no evidence that the Customs network has been compromised.

Nature of the breach

15. **Information Security:** The servers that were stolen are of a type common to any network and are used to process the movement of information between individual computers, hence they are usually located in or near any area where a number of networked computers exist. They are, in effect, powerful computers and thus have monetary or spare-parts value to prospective thieves.
16. Customs does not store any national security classified material on this network. Any electronic national security classified information is received and held in two primary locations. These locations are afforded the highest level of security and are accredited by the Defence Signals Directorate. Access to these facilities is extremely limited. They are contained within a permanently guarded and alarmed building and are protected by at least five levels of security: building access control; guards; floor access control; unit access control and an immediate response alarm system.
17. The computer room that was accessed also contained other EDS equipment and stores, including two other file servers. To date the investigation has not revealed any intrusion into the Customs system from this other equipment.

18. **Physical Security:** Clearly there was a breach of security that allowed unauthorised access to a restricted area. Prima facie this has occurred because the access procedure was not adequate. Customs, which has over 200 separate premises, is reviewing the security of restricted areas and will implement measures to ensure this event is not repeated.
19. All EDS staff working on the Customs account are security cleared by Customs. These staff are issued an identity and access card in a similar manner to Customs officers. However, EDS sub-contracts some of its work and although regular sub-contractor staff are also cleared and issued with a pass, specialist

sub-contractors who might only attend Customs premises infrequently are not cleared and must be escorted.

20. In this incident it appears that the procedure for allowing access by technicians to the computer was to have them sign in and then give them the access card to the computer room, without an escort.
21. The access card only gives access to the computer room, not to other parts of the Customs building. The access card has been disabled and procedures for access to the computer room have been changed.
22. Customs has started discussions with EDS to work out procedures to verify the authenticity of any uncleared sub-contractors entering Customs premises in future.
23. In the meantime, all Customs staff have been reminded that all visitors, including tradespersons and technicians, must be signed in and escorted at all times.
24. Regional Security Advisors are undertaking a further review of the security arrangements of all Customs premises.

Notification to other Agencies

25. When this incident occurred Customs made every effort to determine the extent of potential compromise as quickly as possible. Customs was satisfied at the time, and to date the investigation has not shown otherwise, that other agencies' information had not been compromised.
26. All external agencies with direct access to PACE, Customs passenger processing system, were notified on 28 August, at the same time as Customs users that they had to change their password. The AFP, ASIO, ACC, and DFAT were all called and given a brief explanation of the incident.
27. DIMIA has about 150 users of PACE at airports and all these users also were involved in the password change procedure.

Conclusion

28. Customs adopted a deliberate and methodical approach to ascertaining details of the breach, determining its consequences, eliminating any potential compromise, requesting the assistance of Australian Government experts and confirming its initial views through investigation.
29. The investigation of both the offence and the possible impact on Customs IT system are continuing.
30. The Minister for Justice and Customs has also announced an independent review of the Australian Customs Service security procedures, that will provide the Government with an interim report later this month.

Australian Customs Service
12 September 2003