PARLIAMENTARY JOINT COMMITTEE ON LAW ENFORCEMENT

Examination of the ACC Annual Report

Question on notice:

Question No. 3
The Daily Telegraph reported on 28 February 2012 on an apparent increase in the number of security breaches by staff members of the Australian Crime Commission. The committee would appreciate a response to this report, together with an explanation of the steps taken to reverse this trend.

Response
The Australian Crime Commission (ACC) places great importance on the security of its premises, people and information.

When incidents occur, appropriate action is taken in accordance with Australian Government guidelines on security management (Protective Security Policy Framework).

The ACC raises awareness of security requirements through induction, training and internal communication to staff. This security regime is supported by internal policies and procedures which accord with the Commonwealth Government Protective Security Regime. Security risk assessments are undertaken and inform agency security risk management. A Secret ICT network has being deployed across the ACC to further enhance the ACC security environment.

The ACC has a positive culture of staff self-reporting security incidents, irrespective of the disciplinary action that may result. This culture is supported by a rigorous regime of awareness-raising and education within the agency. When security breaches do occur they are reported and investigated accordingly and should there be any trends of concern, briefings are released across the ACC and changes incorporated to training and awareness. The experience of other agencies is that the reported security incidents may well increase as staff become more aware of security related requirements and the reporting framework.

The media report indicated that there had been 72 security incidents since 2007, which relates to the number of documents provided under a freedom of information (FOI) request.

The total number of incidents contained in the documents released under this FOI was 62 and a breakdown is as follows:

- 2007 – 2
- 2008 – 8
- 2009 – 13
- 2010 – 21
- 2011 – 18

There were a range of incidents, some of which were beyond the control of the ACC and the staff member. For example, 80 per cent of these were lost or stolen security passes or assets, some resulting from houses being burgled. 10 per cent were security breaches or contravention of policy which occurred within the ACC with no external loss of information. Four of the cases were more serious relating to loss of information, or in one case a weapon, of which three

resulted in code of conduct breaches. Code of conduct action is taken in the more serious cases where there may be an element of negligence or intent.

While the number of security breaches is higher than the ACC would like, the ACC would much prefer to know of security breaches, and be in a position to mitigate the risk and put in place strategies for the future. It would be far worse to have little or no reports of security breaches, which may appear positive at face value, but which may in fact mask serious security issues.

It is important to read these figures in the broader context of the ACC's culture of compliance, which has been recognised by the Commonwealth Ombudsman:

The agencies [including the ACC] showed a strong culture of compliance and a high standard of record keeping.[1]

The ACC will continue to be vigilant about security and is continually improving risk assessment, monitoring, investigation and review and internal awareness raising.

[1] Commonwealth Ombudsman report, *Report to the Attorney-General on the results of inspections of records under s 55 of the* Surveillance Devices Act 2004, September 2011, <http://www.ombudsman.gov.au/files/surveillance_devices_2011.pdf>