

# RECOMMENDATIONS

## Chapter 2

### **Recommendation 1** **19**

The Committee recommends that the House of Representatives Committee on Communications, Information Technology and the Arts examine the regulation of Internet Service Providers, including codifying the jurisdictional and evidentiary matters involving material which is transmitted or held by the Provider.

## Chapter 3

### **Recommendation 2** **31**

The Committee recommends that the Government investigate partnerships for establishing a multimedia public education campaign on the risks associated with and the safe use of information technology by children, including parental supervision.

### **Recommendation 3** **35**

The Committee recommends that the Commonwealth Attorney-General liaises with the State and Territory Attorneys-General to ensure that priority is given to the development and implementation of consistent offence and evidence legislation in relation to cybercrime, which is in accordance with Australia's international obligations.

### **Recommendation 4** **35**

The Committee recommends that as part of its legislative package to detect and prosecute those who use information technology for the trade of child pornography, the Government introduce a new offence relating to luring and grooming children for sexual purposes.

## Chapter 4

### **Recommendation 5** **40**

The Committee recommends that the Australian Crime Commission in conjunction with the Australian High Tech Crime Centre investigate the provision of general information on fraud trends to financial institutions through a secure subscription based service.

### **Recommendation 6** **49**

The Committee recommends that the Australian Crime Centre, in consultation with the Australian High Tech Crime Centre (AHTCC), Austrac and other law enforcement agencies give priority to developing a national intelligence gathering strategy for cybercrime in the banking industry. Further the ACC should seek to fill any gaps in intelligence holdings that are identified.

**Chapter 6****Recommendation 7** **65**

The Committee recommends that the Government include in its cybercrime strategy, directed training for law enforcement agencies, and the development of a whole of government approach in which individuals can gain expertise which can be shared between those agencies.

**Recommendation 8** **66**

The Committee recommends that the Australian Crime Commission continue its current level of involvement in cybercrime investigation, and intelligence gathering, as well as further developing its international liaison role.

**Recommendation 9** **66**

The Committee recommends that the Australian Crime Commission ensure its information sharing strategies, including liaison with the Australian High Tech Crime Centre, maximise the opportunities for giving and receiving accurate and timely information about cybercrime methods and technology.

**Recommendation 10** **67**

The Committee recommends that the Australian Crime Commission seek out opportunities to participate in appropriate public/private sector cybercrime projects, to promote the sharing of information, and the efficient prevention and investigation of cybercrime offences.

**Recommendation 11** **68**

The Committee recommends that the Australian High Tech Crime Centre act as a clearing house for information on cybercrime, in order to explore initiatives to combat it.