SUBMISSION NO. 2

SOUTH AUSTRALIA POLICE
KEEPING SA SAFE

Your Ref:	
Our Ref:	ESB09/013396
Enquiries:	Detective Superintendent Jim Jeffery
Telephone:	08 8172 5034
Facsimile:	

Mr Jerome Brown
Acting Committee Secretary
Standing Committee on Communications
PO Box 6021 Parliament House
CANBERRA ACT 2600

June 2009

Dear Mr Brown,

I refer to your letter of 26 May 2009, inviting South Australia Police (SAPOL) to provide a submission to the House of Representatives Standing Committee on Communications into cyber crime and its impact on consumers.

South Australia Police have a small Electronic Crime Section comprised of a manager, five investigators and four electronic evidence specialists. The investigative arm is responsible for:

- The investigation of higher level electronically enabled crime;
- Providing investigational support and / or advice to other SAPOL investigators;
- Providing preventative and security advice to members of the public; and
- Developing and / or disseminating contemporary preventative initiatives to the community.

The following broad comments are provided for consideration by the Committee:

The nature, prevalence and future of technology-enabled crime

The nature and prevalence of e-security risks and impact of technology enabled crime is well documented in two recent documents produced by the Australian Institute of Criminology:

- *The Australian Business Assessment of Computer User Security: a national survey*,[1] examines the prevalence and nature of computer security incidents experienced by Australian businesses and discusses the vulnerability of some systems and the cost, types and effectiveness of prevention mechanisms. It is recommended that the enquiry considers the 4 page Executive Summary of this publication.

[1] Australian Institute of Criminology Research and Public Policy Series 102, *The Australian Business Assessment of Computer User Security*, (Kelly Richards), 2009

- *The future of technology-enabled crime in Australia* (6 pages)[2] succinctly describes in non-complicated terms the prevalence, impact and nature of technology based crimes including the types of viruses and Trojans. Whilst this entire document is highly relevant to the terms of reference, the conclusion summarises the current issues and provides recommendations for the future:

  "The prosecution and judicial disposition of cases involving technology-enabled crime will continue to raise key issues faced by police and prosecutors. These include the need for legislative reforms as a result of the emergence of new offences, criminal complicity, jurisdictional issues (whether jurisdiction exists and the problem of concurrent jurisdiction), complex and novel arguments relating to admissibility of evidence or the exercise of discretion, novel defences and defence arguments and appropriate sentences for convicted offenders.

  There is no single all-encompassing answer to responding to technology-enabled crime. Countering these risks is a multi-dimensional challenge and requires effective coordination and collaborative efforts on the part of a wide range of government and private sector entities. Possible directions for action include:

  - *engaging the ICT security industry in the design of secure software and hardware*
  - *establishing public-private sector partnerships and information sharing initiatives*
  - *establishing task forces dedicated to the investigation and prosecution of technology-enabled crime cases*
  - *enhancing the training and educational capabilities of police, prosecutors and IT professionals.*

  Technical assistance to less ICT-advanced jurisdictions will also be essential. This will help not only to minimise the development of technology-enabled crime within these locations, but also to enable assistance to be provided for the investigation of increasingly cross-jurisdictional technology-enabled crimes. Developing a culture of security for information systems and networks is of primary importance, and this can be achieved through coordinated efforts by both government and private sector organisations. If these efforts are successful, the development of new forms of technology-enabled crime in the future will be minimised."

Prevention & Awareness

Despite enhanced efforts from law enforcement and Government agencies such as the Australian Competition and Consumer Commission (ACCC), the basic e-security message does not appear to be effectively getting through to the Australian community. Whilst the vulnerability of the elderly is concerning, it is disturbing that even prudent and experienced business persons allow themselves to fall victim to easily prevented scams and technology enabled crimes.

Whilst law enforcement and key Government agencies produce a variety of prevention and education initiatives there is limited information sharing or collaboration which can contribute to ineffectiveness and inefficiencies. Very low levels of cross-portfolio and inter-jurisdictional coordination exists. For example a key collaboratively based marketing opportunity was missed through SAPOL not

[2] Australian Institute of Criminology, Trends & Issues paper No. 341, *The future of technology-enabled crime in Australia,* (Kim-Kwang Raymond Choo, Russell G Smith and Rob McCusker, July 2007

being advised of the two week ACCC initiated anti-scam campaign held earlier this year.

There is currently no structured or coordinated framework for Australian law enforcement agencies to collaboratively develop and implement preventative initiatives. National multi-agency initiatives are rarely developed and implemented. Crime prevention and education is one of the key four objectives of The Australian High Tech Crime Centre (AHTCC). Given that the AHTCC is an operational arm of the Australian Federal Police, the prevention and education programs are predominately implemented within Australian Capital Territory and regional New South Wales.

The Australian and New Zealand Policing Advisory Agency (ANZPAA) recently recommended and endorsed the re-establishment of the ANZPAA E-Crime Investigation Managers Committee (AEIMC). Prevention and Awareness coordination is likely to be considered by this group.

It is widely recognised that security enhancement, prevention, education and disruption of technology-enabled crime is more effective than investigation based strategies. This strategy is accepted on the understanding that the majority of technology-enabled crimes committed against Australians originate off shore, with very minimal prospects of identifying and apprehending the offenders. A lack of legislative consistency across international jurisdictions and limited capabilities of law enforcement agencies to take action against off shore offenders, minimises the effectiveness of investigations.

Training and capability development

There is currently a lack of consistency in the frequency and levels of training provided to law enforcement detectives involved in investigating technology-enabled crime. Maintaining suitable levels of training is expensive. The level of training provided is usually dependant on the availability of funding which varies considerably across law enforcement agencies. The skills and competencies of investigators have to be continually upgraded to be able to understand new technology and the investigative techniques required. Whilst it is anticipated that the AEIMC will assist in standardising and coordinating some training requirements, there is a need for minimum standards to be set and processes established to ensure that law enforcement agencies maintain a capacity to investigate technology-enabled crime.

Australian law enforcement agencies did attempt to implement a collaborative approach to preventing and investigating technology enabled crime through the formation of the AHTCC in 2003. Most State based law enforcement agencies provided staff and some funding to the AHTCC until it was disbanded in 2007. The AHTCC did succeed in establishing the Joint Banking Task Force and increasing the capabilities of detecting and investigating some forms of technology-enabled crimes such as the down loading of child pornography. Conflicting investigational priorities and an emphasis of addressing Commonwealth priorities to the detriment of State based investigations contributed to the eventual disbandment of the AHTCC in 2007.

Any future proposal to re-establish a National coordination centre would need to ensure that sufficient Commonwealth funding is provided to enable all State based participants to receive the same training and have equal access to non law enforcement expertise. Governance would need to be provided by all States and the AFP, particularly in terms of setting investigational priorities. Alternatively, any new model could focus on providing skills support, training and the development and coordination of awareness and prevention as opposed to conducting investigations.

It is anticipated that the exchange of information in relation to the latest technology-enabled crime trends and methods will be encouraged through the AEIMC as currently there is no coordinated medium for information to be exchanged. The establishment of a National capability register will also be a priority of the AEIMC, enabling law enforcement agencies to acquire a list of available experts that are available and how they can be sourced.

I trust that this submission is useful to the Standing Committee and invite you to contact Detective Superintendent Jim Jeffery, Officer In Charge, Commercial & Electronic Crime Branch on 08 8172 5034 should you have any queries relating to this submission.

Yours Sincerely,

(Tony Harrison)
ACTING DEPUTY COMMISSIONER OF POLICE