AFP Submission to the Senate Legal & Constitutional Affairs Committee inquiry into the *Telecommunications (Interception and Access) Amendment Bill 2008*

Extension of Sunset Clause on network protection exemptions in the Telecommunications (Interception & Access) Act 1979

AFP network protection and professional standards needs

In response to the growing importance of email as a business communication tool, the Australian Federal Police (AFP) has established a range of network security systems to protect its IT systems at the gateway to the internet from virus, spam, hackers and denial of service attack. The AFP's approach to network security like other government agencies is mandated by the Protective Security Manual and ACSI33. In accordance with these guidelines gateway security requirements for content and message filtering exist and are in place within the AFP.

In addition to this network security function, the AFP uses the same technology to maintain the AFP professional standards regime through monitoring emails to detect inappropriate content and manage information that its personnel forwards and receives. Maintenance of the AFP's professional standards is integral to its ability to provide ethical and accountable policing services to the Australian Government and the community.

The current internal AFP policy on email has been in place since 2003. It sets out for AFP employees, the organisation's expectations for the work related use of email and appropriate personal use as well outlining how the email system is protected and monitored, including an explanation of IT auditing and access procedures in relation to emails sent to and from the AFP network. The policy also clearly states the consequences for AFP employees who breach this policy.

If there is evidence that an AFP appointee is sending emails with inappropriate or suspicious content, it is formally entered onto the AFP's Complaint Recording and Management System (CRAMS). Inappropriate use of email is a breach of the AFP Code of Conduct and the National Guideline on the Use of Email. All complaints are investigated, with more serious breaches investigated by Professional Standards.

Standard network protection practice

It is standard government agency and business enterprise practice for the gateway to protect holdings. Emails can carry with them malicious code (eg, viruses, worms, Trojans) which enables a hacker to install a back door to an IT system, potentially giving them unlimited access to an organisation's entire information system.

AFP IT Security personnel are analogous to 'bomb technicians' in that they determine the danger of the content of the package and subsequently determine the path the package should take (sent on, stopped or deleted). Human intervention is essential in the process of monitoring email traffic into and out of the AFP for the protection of information systems.

In the case of the AFP corporate network, the gateway protects operational, intelligence, administrative and related information and works as follows:

- Incoming email is received and examined by email filtering software.

- If the email is not blocked (is identified as not containing an anomaly) it is forwarded to the recipient. An archive copy of the email is the created.

- If an anomaly is detected (eg, virus, inappropriate image, executable file etc) the email is quarantined and the employee is notified. At this point a copy of the email is archived.

- Employees may request release of quarantined emails.

- If no request for release is received the email is automatically deleted after a specified period (usually 7 days).

Previous legislative amendments

The current exemption, which was first introduced as a government amendment to the *Telecommunications (Interception) Amendment Bill 2006*, was introduced with a two year sunset clause. It was not included in the original Bill or raised during the Senate Committee inquiry because it had not received final policy approval at that time. This amendment was the result of additional analysis of the Bill by the AFP and the Attorney-General's Department to ensure that current AFP network administration and protection practices, including those related to the support of its professional standards regime outline above, would continue to have appropriate legal support once the proposed amendments commenced.

Need for the sunset clause to be extended

The proposed 18-month extension of the existing network protection provisions will ensure the AFP and other agencies covered by the exemption can continue to protect their networks while a comprehensive long-term solution is developed.

The AFP is working with the Attorney-General's Department on the development of that solution and will support it in the consultation process that is required to address the issues associated with other networks as well as the laws of other jurisdictions in Australia.

<u>Device based named person warrant amendments</u>

Device-based named person warrants were introduced to the interception regime in the *Telecommunications (Interception) Amendment Act 2006* to address the gap identified in the interception regime by the Review of Regulation of Access to Communications undertaken by Mr Anthony Blunn AO (the Blunn Review). The Blunn Review identified that an interception solution was required to deal with the proliferation of SIM cards, the tendency for criminals to evade interception by rotating SIM cards through multiple hand sets and the difficulty in identifying persons who purchased pre-paid SIM cards.

Device-based named person warrants were introduced to complement the service-based named person warrant regime and allow interception to occur on the basis of a uniquely identified device rather than the telecommunication service such as the SIM card or email account. At this time, provisions were also introduced (sections 16A and 60(4A) of the *Telecommunications (Interception & Access) Act 1979*) to align device-based named person warrants with service-based named person warrants and allow devices to be added to warrants

as additional devices became known to investigators after a device-based warrant had been issued.

AFP investigators determine that the device to be intercepted can be uniquely identified and is connected to the person named in the warrant by lawful technical means and by undertaking extensive enquiries with carriers and carriage service providers to. These practices would occur regardless of whether the enquiries were in relation to the initial warrant application or for the purposes of adding further devices to a warrant.

The TIA amendment Bill 2008 aims to clarify the situation that once a device-based named person warrant is issued by an issuing authority, all devices identified as connected to the named person can be intercepted without having to obtain a separate warrant for each device.