Ms Fiona Bowring-Greer
Committee Secretary
Parliamentary Joint Committee on Law Enforcement
PO Box 6100
Parliament House
Canberra ACT 2600

20 November 2012

INQUIRY INTO THE GATHERING AND USE OF CRIMINAL INTELLIGENCE

During evidence before the Committee the Australian Federal Police Association (AFPA) Branch of the Police Federation of Australia made reference to the inquiry conducted by the ICAC into unauthorised release of Government information.

As AFPA National President, I made mention that delays in obtaining essential information/intelligence through official channels created an unauthorised exchange of information/intelligence as it was more efficient and effective in fighting crime and protecting Police officers from harm. Unfortunately this process was open to corruption by some officials/police.

A large number of Commonwealth agencies and Commonwealth officials were identified during the ICAC investigation and I believe this further information may assist the PJC-LE Committee. The ICAC findings and recommendations are very relevant as intelligence and information should be considered the same for the purpose of your inquiry.

During the ICAC inquiry it identified what was colloquially called the *Information Exchange Club*. It noted that:-

- *Well intentioned and sometimes authorised exchange of confidential information was a major contributor to unauthorised release of Government information. Either by law or as a matter of practice, agencies involved in the investigation of crime have access to confidential information held by public authorities. There has also been co-operation among government departments and agencies in exchanging information for other purposes. Unauthorised dissemination of confidential government information resulted.*

- *Official department-to-department arrangements involving designated officers were often replaced by unofficial arrangements between individual officers. Contacts were established at social functions organised for the purpose, apparently with departmental approval.*

- *The use of improper means to meet the perceived need for a free flow of information, can conceal the problem, and delay or prevent discussion of proper means that might be devised.*

What did the ICAC find as a result of its inquiry?

Information that has been held as confidential has generally not been well protected. Rudimentary precautions have not been taken with the systems that have been in place.

Much of that evidence concerned information exchange. Information from the Department of Social Security, the Department of Immigration, and the Australian Customs Service, was released in that way. Some of it found its way onto the illicit market. There was evidence that information from Australia Post and Telecom escaped by the same route.

What did the ICAC recommend in regards to protected information/intelligence?

- *All non public government information should be protected by legislation. Legislation should prohibit its unauthorised release and dissemination. If it is to achieve that, it must be effective at every point in the distribution chain. It needs to focus upon the information and unauthorised dealings in it, rather than incidental circumstances such as computer access or payment.*

- *Some government information is likely to be available to certain persons or classes of person only. Special provisions may be necessary to control it. But basically it should be treated in the same way as publicly available information when sought by those entitled to it, (all information should be made readily, and quickly available) and as protected information in all other respects.*

- *That security of all information storage and retrieval systems be constantly monitored, and where necessary updated and improved.*

- *That access to protected information be strictly limited, and an efficient system maintained to enable the persons responsible for all accesses to be identified. Where personal access codes are used for the purpose, strict security of those codes should be required and maintained. To the extent that it is practical, access through particular codes should be limited to specified terminals or entry points. Systems should be so designed that access is denied on transfer, leave, suspension, or other cessation of need.*

Relevance to this Inquiry

As a result ICAC *Report On Unauthorised Release Of Government Information* in August 1992, free flow of information/intelligence became even more restrictive with government agencies deciding to nominate strict request processes though a limited number of personnel resulting in information/intelligence <u>not</u> being readily and quickly available to those persons appropriately authorised to obtain access to such information/intelligence, stifling the gathering and use of criminal intelligence.

Conclusion

Intelligence sharing between law enforcement agencies and other agencies with relevant intelligence holdings is an integral part of the fight against crime.

As mentioned in evidence the AFPA and the PFA believe that the future of Australian law enforcement is the free flow of criminal intelligence, utilising modern intelligence-sharing technical capability.

Police Officers should be provided with direct real time access to intelligence holdings on operational grounds. Police officers and those they interact with are most at risk when an officer is forced to operate in a situation without proper intelligence regarding the circumstances of the situation.

As mentioned in the PFA submission, *in the context of organise crime investigation and disruption, ACC CEO John Lawler has spoken about the need for real time intelligence to fight organised crime, saying that to combat organised crime, intelligence needs to be available within 48 hours of it occurring*[1]. *In the context of frontline policing, direct real time access can be crucial when an operational police officer must act quickly on intelligence, such as dealing with a suspect, or considering a pursuit.*

As mentioned in evidence, many police forces still use central and sometimes manual processes for intelligence sharing, which slows down the intelligence flow to operational frontline police officers. This is inefficient, time consuming, and potentially dangerous to operational police and those they interact with.

The current dissemination processes and practices have already been identified by the ICAC in its 1992 *Report on Unauthorised Release of Government Information,* to encourage the use of improper means to meet the need for a free flow of information, which subsequently creates a corruption risk.

Corruption, privacy and integrity concerns relating to police directly accessing real time intelligence holdings on operational grounds is best addressed by 'electronic data tracking' capabilities, which current technology can provide, if applied to a uniform, electronic system.

I trust that this additional information is of assistance to the Committee.

Yours sincerely

Jon Hunt-Sharman
National President
Australian Federal Police Association

[1] John Lawler, Presentation to the 10th Anniversary National Security Australia Conference 2012 ACC Speeches and Presentations Tue, 13/03/2012.