PARLIAMENTARY JOINT COMMITTEE ON THE AUSTRALIAN COMMISSION FOR LAW ENFORCEMENT INTEGRITY

AUSTRALIAN FEDERAL POLICE

**Question No. 1**

**Senator Cameron asked the following question at the hearing on 19 August 2011:**

**Senator CAMERON:** I have a number of questions but we are running out of time so I might just put some questions on notice, if that is okay. You say on page eight at clause 31 that the suite of tools available for integrity testing is limited. Is there any chance you could give us a supplementary submission or an answer to this question about what is the limit that you see here? You make the statement, but there is no detail. I would like to get some detail.

**The answer to the honourable senator's question is as follows:**

The Australian Federal Police (AFP) submission to the Parliamentary Joint Committee on the Australian Commission for Law Enforcement Integrity inquiry into integrity testing indicated the availability of covert policing powers for integrity testing.

The AFP submission notes that in many integrity test scenarios, it may be necessary to use undercover operatives using assumed identities, or to rely on other covert police powers such as controlled operations, the use of surveillance devices or access to telecommunications. The AFP submission indicated that the availability of covert policing powers would depend on whether the circumstances of the integrity test met the threshold requirements for the use of those powers. Where the integrity test did not meet the threshold, the suite of tools available for integrity testing would be limited.

<u>Assumed identities</u>

2. An assumed identity is a false identity used for the purpose of investigating an offence for intelligence gathering purposes. An assumed identity provides an officer with the appropriate 'cover' to investigate or gather information without prejudicing the operation (or his or her safety). In some circumstances, an integrity test scenario might require the use of undercover operatives, using an assumed identity.

3. An assumed identity can be used without authorisation under the relevant Commonwealth, State or Territory legislation. However, without authorisation under the relevant law, the officer does not have any of the powers or protections conferred by legislation. Importantly, the officer will not be able to obtain 'evidence' to substantiate the assumed identity (such as a passport). This is because it will generally be an offence for documents to be issued under a false name; assumed identities legislation provides protection from such criminal liability.

4. Persons subject to an integrity test are in a unique position to confirm the cover story of an operative. Such persons are familiar with investigative methodologies, and have access to government databases and police indices. Therefore, the ability to use an *authorised* assumed identity and evidence to support that identity can be essential to conducting a successful integrity test.

5. The relevant legislation for assumed identities at the Commonwealth level is Part IAC of the *Crimes Act 1914*. Relevant to the AFP, under Part IAC an assumed identity can be authorised where the authorising officer is satisfied, on reasonable grounds, that the assumed identity is necessary for one or more of the following purposes:

- the investigation of, or intelligence gathering in relation to, criminal activity;
- the exercise of powers and performance of functions for the National Witness Protection Program; and
- the training of persons for, and the administrative support of, those purposes.

Controlled operations

6. Controlled operations legislation governs circumstances in which it is necessary for undercover operatives to commit offences in order to obtain evidence and conceal their law enforcement role. The relevant legislation for controlled operations at the Commonwealth level is Part IAB of the Crimes Act.

7. Under Part IAB, the undercover operative will be protected from criminal liability for his or her conduct provided that, among other things:

- the operative acted in accordance with the authorisation for the controlled operation;
- the operative did not intentionally induce a person to commit an offence the person would not otherwise have intended to commit; and
- the conduct does not involve the operative engaging in any conduct likely to cause the death of or serious injury to a person, or the commission of a sexual offence against any person.

8. Part IAB provides that, in determining whether evidence should be admitted or excluded in any proceedings, the fact that the evidence was obtained as a result of a person engaging in criminal activity is to be disregarded if both:

- the person was a participant in an authorised controlled operation authorised, acting in the course of the controlled operation; and
- the criminal activity was controlled conduct.

9. Under Part IAB, a controlled operation can only be authorised where the authorising officer is satisfied, on reasonable grounds, of certain matters. Relevantly, the authorised officer must be satisfied that:

- a serious Commonwealth offence or a serious State offence that has a federal aspect has been, is being or is likely to be committed; and
- that the nature and extent of the suspected criminal activity are such as to justify the conduct of a controlled operation.

"Serious offences" are defined by reference to certain offence types carrying a penalty of three or more years imprisonment; other offences carrying a lower penalty are also prescribed.

Surveillance devices

10. Surveillance devices are an important covert investigative tool. The relevant legislation for the use of optical, listening and data surveillance devices at the Commonwealth level is the *Surveillance Devices Act 2004* (the SD Act).

11. Under the SD Act, a warrant is generally required for the use of a surveillance device. A warrant is not required in certain circumstances, for example, where the use of a camera in a public place or on private property with the consent of the occupier. The issuing officer for a surveillance device warrant must be satisfied that there are reasonable grounds to suspect that:

- one or more relevant offences have been, are being, are about to be, or are likely to be, committed;
- an investigation into those offences is being, will be, or is likely to be, conducted; and
- the use of a surveillance device is necessary in the course of that investigation for the purpose of enabling evidence to be obtained of the commission of the relevant offences or the identity or location of the offenders.

A "relevant offence" is defined a Commonwealth offence, or State offence with a federal aspect, that has a penalty of three or more years imprisonment; other offences are also prescribed.

Telecommunications data and content

12. Access to telecommunications, is regulated by the *Telecommunications (Interception and Access) Act 1979* (TIA Act). Telecommunications data (information about the process of a communication, such as when an email was sent) is an important law enforcement tool that can confirm intelligence or provide new leads. The content of telecommunications (such as an email, SMS or a conversation during a phone call) can also provide investigative leads, and vital evidence of an offence. There are different threshold tests depending on whether telecommunications data or the content of a telecommunication is being accessed. Generally speaking:

- Historical telecommunications data (data that came into existence before the authorisation) can be accessed when it is reasonably necessary for the enforcement of the criminal law (ie any offence). A higher threshold test (offences that has a penalty of at least three years imprisonment) applies to accessing prospective data.

- The content of stored communications (ie SMS, email) can be accessed under warrant where the issuing officer is satisfied that information that would likely be obtained by accessing the stored communications would be likely to assist with the investigation of a serious contravention (generally an offence that has a penalty of at least three years imprisonment).

- A telephone interception warrant can be issued where the issuing officer is satisfied that information that would likely be obtained by intercepting the communications would be likely to assist with the investigation of a serious offence (generally offences of a certain type, usually carrying a penalty of over seven years imprisonment).

Whether covert policing powers would be available for integrity testing

13. Whether the covert policing powers described above would be available for integrity testing purposes will depend on the conduct triggering the integrity test.

14. As described above, covert policing powers are generally only available for the investigation of criminal activity and in some cases is restricted to the investigation of serious offences. Accordingly, covert policing powers are not available for the investigation of professional misconduct that is not a criminal offence (eg an AFP member being rude to a member of the public or an AFP member who fails to comply with administrative procedures).

15. When approving the use of covert policing powers, the authorising or issuing officer usually needs to be satisfied (to an objective standard) that a criminal offence has, is or will be committed. Where there is only limited intelligence indicating criminal activity, this may not be sufficient to meet the threshold test.

16. Where there was evidence of a criminal offence, the AFP would generally conduct a criminal investigation rather than conducting an integrity test. There may be some circumstances, however, in which it is not clear whether the particular conduct was intentional (and therefore an indicator of criminal activity), or an innocent oversight or an IT systems failure (and therefore would not meet the threshold for using covert police powers).

17. For example, there could be intelligence indicating that a particular AFP member is failing to register seizures of controlled drugs in accordance with AFP internal governance requirements. There could also be separate intelligence that unspecified AFP members are involved in drug trafficking. This information, however, may not be sufficient to meet the threshold for the use of covert policing powers as part of a criminal investigation. Access to covert policing powers, such as a controlled operation, would be necessary as illicit substances would be involved.

18. Given the potential seriousness of the combined information, an integrity test, unpinned by a legislative framework that enabled access to covert powers based on different threshold tests, could provide valuable information about the cause of the failure to register the drugs properly. However, current AFP professional standards processes allow further intelligence to be gathered in this scenario which could in any event yield enough information to pursue a criminal investigation, or pursue a professional standards investigation which could include immediate suspension if warranted or identify the failure to register drugs in that particular situation as an oversight.

19. An integrity test might reveal systemic corruption in which seizures of controlled drugs seizures are not being registered and are in fact being sold by AFP members contrary to the trafficking drugs offences in the *Criminal Code* (Cth), which carry serious penalties of 10 years and up to life imprisonment. The AFP would then conduct a criminal investigation, with a view to prosecuting the AFP members involved. The AFP could also take action to terminate the employment of those members.

20. An integrity test might, however, simply point to a lack of sufficient knowledge of the correct exhibit registration procedures, which could be addressed through further training and supervision of the AFP member. This would be consistent with the AFP's approach to managing minor conduct matters through the use of remedial measures designed to improve the AFP member's performance of their duties. Alternatively, an integrity test might indicate that the AFP member is in fact entering the details about the seizure correctly, but there is a problem with the exhibit database and as such the seizure does not appear to be recorded. The corrective action in this case would be to develop an IT solution to address the problem.