Australian Government

Attorney-General's Department

Criminal Justice Division

Parliamentary Joint Committee on the

Australian Commission for Law Enforcement Integrity

Inquiry into Integrity Testing

Attorney-General's Department Submission

August 2011

Attorney-General's Department submission to the Parliamentary Joint Committee on the Australian Commission for Law Enforcement Integrity

Inquiry into Integrity Testing

The Attorney-General's Department (AGD) is pleased to provide this submission to the Parliamentary Joint Committee (PJC) on the Australian Commission for Law Enforcement Integrity (ACLEI) for the purposes of its Inquiry into Integrity Testing. This submission focuses on legislative issues that may be relevant to the consideration of a possible Commonwealth law enforcement integrity testing framework.

1. Commonwealth law enforcement integrity

The Commonwealth's approach to law enforcement integrity is multi-layered and includes:

- internal agency governance, integrity and professional standards arrangements
- external accountability by ACLEI (for the Australian Crime Commission (ACC), Australian Federal Police (AFP), and the Australian Customs and Border Protection Service (Customs)) and, more broadly, by the Commonwealth Ombudsman
- oversight by Government, including Ministers, Cabinet and the Prime Minister, and
- oversight by Parliament, including Parliamentary Committees.

2. Integrity testing

Integrity testing is a specific method of detecting and investigating corruption or misconduct that is not currently undertaken by Commonwealth agencies. Within the law enforcement context, integrity testing refers to the act of covertly placing an officer in a simulated situation designed to test whether they will respond in a manner that is illegal, unethical or otherwise in contravention of the required standard of integrity. The test must provide the subject with an equal opportunity to pass or fail the test. Depending on its severity, the consequences of failing integrity tests can include disciplinary action, termination of employment or criminal charges.

Integrity testing can be used to test a range of matters from relatively minor misconduct (that may or may not be illegal) to corruption of a serious criminal nature. The potential application of integrity testing for law enforcement agencies will depend on a number of considerations, including the nature of their roles, responsibilities, activities and risk profile.

Integrity testing can be a costly and resource intensive process. The conduct of integrity testing may in some instances involve participants in the testing scenario engaging in controlled illegal activity. Integrity testing can be conducted in many ways, but is generally carried out on either a random or targeted basis.

Random integrity testing involves the testing of officers who are not under suspicion for any specific corruption or misconduct. Its primary goal is deterrence from engaging in such behaviour. Random integrity testing can be applied widely within an organisation, or only to specific areas or units that may be subject to a higher risk of corruption. Random integrity testing is not an investigation, although its outcomes may lead to one.

Targeted integrity testing involves the selection of officers for testing based on intelligence gathered by other methods. Targeted integrity testing can be conducted in relation to individuals or groups. Its primary goal is to proactively 'catch' or 'clear' the target. Targeted integrity testing can be conducted as part of a formal criminal investigation relating to corruption. Some of the powers that may be used if integrity testing is undertaken where criminal activity is suspected include controlled operations, telecommunications interception and access, surveillance devices and assumed identities.

3. Integrity testing using controlled operations

Conducting integrity testing may sometimes require those arranging the testing to act in a way that would ordinarily be illegal - such as offering bribes or handling illicit substances. If so, controlled operations legislation establishes a regime under which this could occur. Part IAB of the *Crimes Act 1914* (Cth) (the Crimes Act) regulates the use of controlled operations and provides protection to officers involved in conducting those operations.

Part IAB specifically permits ACLEI to authorise controlled operations relating to the investigation of a corruption issue.[1] The AFP and ACC can also authorise controlled operations. Customs can conduct controlled operations if it is authorised by the AFP, ACC or ACLEI.

Purpose of conducting controlled operations

In order to authorise a controlled operation, the authorising officer must be satisfied that certain offences have been, are currently, or are likely to be committed'.[2] Although targeted integrity testing may satisfy this threshold (when it is informed by sufficient intelligence), random integrity testing will not.

Conduct that may give rise to controlled operations

Under Part IAB, a controlled operation may be 'carried out for the purpose of obtaining evidence that may lead to the prosecution of a person for a serious Commonwealth offence or a serious State offence that has a federal aspect'.[3] A serious Commonwealth offence is an offence that is punishable by at least three years imprisonment and involves a prescribed matter, such as bribery or corruption by a Commonwealth officer, fraud or theft.[4] These criteria would capture a number of situations in which integrity testing might be used,

[1] *Crimes Act 1914* (Cth), s 15GF(1)(d).
[2] *Crimes Act 1914* (Cth), s 15GI(2)(a).
[3] *Crimes Act 1914* (Cth), s 15GD.
[4] *Crimes Act 1914* (Cth), s 15 GE(2).

including the receipt of a corrupting benefit and abuse of public office offences under the Commonwealth Criminal Code.[5]

4. Inducement and entrapment

Integrity testing may involve situations where targets are overtly presented with an opportunity for corruption or misconduct, such as being offered a bribe. This type of integrity testing raises potential entrapment and inducement issues.

Authority for a controlled operation cannot be granted if the operation is likely to induce a person to commit an offence that they would not otherwise have intended to commit.[6]

If the outcome of an integrity test is sought to be used as evidence for criminal proceedings, the degree to which the target was induced to commit the offence may result in the evidence being excluded in court. Section 138 of the *Evidence Act 1995* (Cth) gives a court discretion to exclude improperly obtained evidence, which may include evidence obtained through inducement or entrapment.[7] In doing so, the court will weigh the undesirability of admitting evidence obtained in the manner in question against the desirability of admitting that evidence.

If the outcome of an integrity test is sought to be used as the basis of disciplinary action or termination of employment, the principles of procedural fairness would apply to the making of any such decision. This would involve the decision maker being, and appearing to be, free from bias and/or the target receiving a fair hearing before any decision adverse to them is taken.

5. Other legislation relevant to integrity testing

Integrity testing, including integrity testing through controlled operations, may also require the use of other covert investigative powers, such as telecommunications interception, surveillance devices and assumed identities.

Telecommunications interception and access

The *Telecommunications (Interception and Access) Act 1979* (Cth) (the TIA Act) allows the ACC, AFP and ACLEI to intercept and monitor a person's communications in real time. Warrants can be obtained for telecommunications interception if on reasonable grounds an offence has been or is likely to have been committed and the interception information would likely assist in an investigation of that serious offence. A serious offence for the purposes of telecommunications interception includes an offence punishable by at least seven years imprisonment that involves a prescribed matter, including corruption by a Commonwealth officer, theft, abuse of public office and dishonesty offences.

---

[5] Commonwealth Criminal Code, ss 142.1 and 142.2 respectively.

[6] See *Crimes Act 1914* (Cth), ss 15GI(2)(f) and 15HA(2)(c).

[7] See *Ridgeway v the Queen* (1995) 184 CLR 19 at 36-37 per Mason CJ, Deane and Dawson JJ. Also *Robinson v Woolworths Ltd* (2005) 158 A Crim R 546 and *R v Stubbs* [2009] ACTSC 63.

The TIA Act also allows the ACC, AFP, ACLEI, Customs and some other agencies to access stored communications, such as email and SMS messages. Warrants can be obtained for accessing stored communications if on reasonable grounds an offence has been or is likely to have been committed and the information would likely assist in an investigation of a serious contravention. A serious contravention includes all serious offences or any other offence punishable by at least three years imprisonment or 180 penalty units.

The TIA Act also allows the ACC, AFP, ACLEI and Customs to access telecommunications data, such as the date, time, location and duration of phone calls. Data can be accessed subject to an internal authorisation by an appointed authorised officer. The TIA Act enables this information to be accessed on a prospective basis by law enforcement agencies when the disclosure is reasonably necessary for the investigation of offences subject to at least three years imprisonment. The TIA Act also enables this information to be accessed on a historical basis where disclosure is reasonably necessary for the enforcement of the criminal law or a law imposing a pecuniary penalty, regardless of the penalty threshold.

Surveillance Devices

The *Surveillance Devices Act 2004* (Cth) allows the ACC, AFP and ACLEI to use surveillance devices, including optical, listening, data and tracking devices. Warrants can be obtained for surveillance devices if there are reasonable grounds for a suspicion that an offence has been, or is likely to be committed and that offence is punishable by at least three years imprisonment.

Assumed identities

Part IAC of the Crimes Act allows a range of law enforcement agencies to use assumed (i.e. false) identities. Authority to use an assumed identity can be obtained to support an investigation, or gather intelligence in relation to, criminal activity.