Submission No 174

Inquiry into potential reforms of National Security Legislation

Organisation: Australian Commission for Law Enforcement Integrity

Australian Government

Australian Commission for
Law Enforcement Integrity

Parliamentary Joint Committee on Intelligence and Security

Inquiry into potential reforms of National Security Legislation

Submission by the Australian Commission for Law Enforcement Integrity

22 August 2012

1. Introduction

The Australian Commission for Law Enforcement Integrity (ACLEI) welcomes the opportunity to make a submission to the Parliamentary Joint Committee on Intelligence and Security (the Committee) concerning its *Inquiry into potential reforms of National Security Legislation*.

To assist the Committee, Part 2 of this submission provides background about ACLEI's role and responsibilities, and Part 3 provides comments relating to ACLEI's experience as a user of telecommunications-based law enforcement powers and authorities, and as an anti-corruption agency.

2. Role and responsibilities of ACLEI

Establishment

The office of Integrity Commissioner, and ACLEI, are established by the *Law Enforcement Integrity Commissioner Act 2006* (the LEIC Act).

The objects of the LEIC Act (at section 3) are:

> *(a) to facilitate:*
>
> *(i) the detection of corrupt conduct in law enforcement agencies; and*
>
> *(ii) the investigation of corruption issues that relate to law enforcement agencies; and*
>
> *(b) to enable criminal offences to be prosecuted, and civil penalty proceedings to be brought, following those investigations; and*
>
> *(c) to prevent corrupt conduct in law enforcement agencies; and*
>
> *(d) to maintain and improve the integrity of staff members of law enforcement agencies.*

The agencies subject to the Integrity Commissioner's jurisdiction under the LEIC Act are the Australian Crime Commission (ACC), the Australian Customs and Border Protection Service, the Australian Federal Police (AFP) and the former National Crime Authority.

Role

ACLEI's primary role is to investigate law enforcement-related corruption issues, giving priority to systemic and serious corruption. ACLEI also collects intelligence about corruption in support of the Integrity Commissioner's functions.

The Integrity Commissioner must consider the nature and scope of corrupt conduct revealed by investigations, and report annually on any patterns and trends concerning corruption in law enforcement agencies.

ACLEI also aims to understand corruption and prevent it. When, as a consequence of performing his or her functions, the Integrity Commissioner identifies laws of the Commonwealth or the administrative practices of government agencies with law enforcement functions that might contribute to corrupt practices or prevent their early detection, he or she may make recommendations for these laws or practices to be changed.

Under section 71 of the LEIC Act, the Minister may also request the Integrity Commissioner to conduct a public inquiry into all or any of the following:

- a corruption issue;
- an issue about corruption generally in law enforcement; or
- an issue or issues about the integrity of staff members of law enforcement agencies.

Independence

ACLEI is a statutory authority, and part of the Attorney-General's portfolio. The Minister for Home Affairs, Minister for Justice is responsible for ACLEI.

Impartial and independent investigations are central to the Integrity Commissioner's role. Although the Minister may request the Integrity Commissioner to conduct public inquiries, the Minister cannot direct how inquiries or investigations will be conducted.

The LEIC Act contains measures to ensure that the Integrity Commissioner and ACLEI remain free from political interference and maintain an independent relationship with government agencies. Accordingly, the Integrity Commissioner:

- is appointed by the Governor-General and cannot be removed arbitrarily;
- is appointed for up to five years, with a maximum sum of terms of seven years;
- can commence investigations on his or her own initiative; and
- can make public statements, and can release reports publicly.

Receiving and disseminating information about corrupt conduct

The LEIC Act establishes a framework whereby the Integrity Commissioner and the agency heads can prevent and deal with corrupt conduct jointly and cooperatively. The arrangement recognises both the considerable work of the agencies in the Integrity Commissioner's jurisdiction to introduce internal corruption controls (including detection and deterrence-focussed mechanisms) and the continuing responsibility that the law enforcement agency heads have for the integrity of their staff members.

An important feature of the LEIC Act is that it requires the head of an agency in ACLEI's jurisdiction to notify the Integrity Commissioner of any information or allegation that raises a corruption issue in his or her agency (section 19).

The LEIC Act also enables any other person, including members of the public or other government agencies or the Minister, to refer a corruption issue to the Integrity Commissioner.

Further, ACLEI is authorised under the *Telecommunications (Interception and Access) Act 1979* to receive information about any corruption issue involving an agency within the LEIC Act jurisdiction that may be identified by other integrity agencies or law enforcement agencies as a result of their telecommunications interception activities.

Special legislative arrangements make it lawful for "whistleblowers" to provide information about corruption direct to ACLEI. The LEIC Act provides for ACLEI to arrange protection for witnesses.

The Integrity Commissioner may disclose information to the head of a law enforcement agency, or other government agency, if satisfied that, having regard to the functions of the agency concerned, it is appropriate to do so.

The Integrity Commissioner is exempt from the operation of the *Privacy Act 1988*, reflecting the importance of ACLEI's collection and intelligence-sharing role.

Investigation options

The Integrity Commissioner decides independently how to deal with any allegations, information or intelligence about corrupt conduct concerning the agencies in ACLEI's jurisdiction.

The Integrity Commissioner is not expected to investigate every corruption issue that arises in Commonwealth law enforcement. Rather, the Integrity Commissioner's role is to ensure that indications and risks of corrupt conduct in law enforcement agencies are identified and addressed appropriately.

The Integrity Commissioner can choose from a range of options in dealing with a corruption issue. The options are to:

- investigate the corruption issue;
- investigate the corruption issue jointly with another government agency;
- refer the corruption issue to the law enforcement agency for internal investigation (with or without management or oversight by ACLEI) and to report findings to the integrity Commissioner;
- refer the corruption issue to another agency, such as a State integrity agency, the AFP, or another government agency, for investigation; or
- take no further action.

Section 27 of the LEIC Act sets out the matters to which the Integrity Commissioner must have regard in deciding how to deal with a corruption issue.

With these matters in mind, the Integrity Commissioner will investigate when there is advantage in ACLEI's direct involvement. Under the LEIC Act, the Integrity Commissioner must also give priority to serious or systemic corruption.

Accordingly, the Integrity Commissioner gives priority to corruption issues that may:

- involve a suspected link between law enforcement and organised crime;
- bring into doubt the integrity of senior law enforcement managers;
- relate to law enforcement activities that have a higher inherent corruption risk;
- warrant the use of the Integrity Commissioner's information-gathering powers, including hearings; or
- would otherwise benefit from independent investigation.

ACLEI also prioritises corruption issues that have a nexus to the law enforcement character of the agencies in its jurisdiction, having regard to the objects of the LEIC Act.

Investigation powers

A challenge facing ACLEI is that law enforcement officers subject to investigation by the Integrity Commissioner are likely to be familiar with law enforcement methods, and may be skilled at countering them in order to avoid scrutiny. As a consequence, ACLEI has access to a range of special law enforcement powers.

The key investigative powers available to the Integrity Commissioner and ACLEI are:

- notices to produce information, documents or things;
- summons to attend an information-gathering hearing, answer questions and give sworn evidence, and/or to produce documents or things;
- intrusive information-gathering (covert);
    - telecommunications interception;
    - electronic and physical surveillance;
    - controlled operations;
    - assumed identities;
    - scrutiny of financial transactions; and
    - access to specialised information databases for law enforcement purposes;
- search warrants;
- right of entry to law enforcement premises and associated search and seizure powers; and
- arrest (relating to the investigation of a corruption issue).

It is an offence not to comply with notices, not to answer truthfully in hearings, or otherwise to be in contempt[1] of ACLEI.

[1] See, section 96B (Federal Court or Supreme Court to deal with contempt), *Law Enforcement Integrity Commissioner Act 2006.*

3. ACLEI's experience

The use in modern society of telecommunications, including internet-based communications and mobile devices, is ubiquitous. It follows that their use as tools for arranging or coordinating the commission of crimes is also commonplace. It may be argued that advances in technology have facilitated the rapid expansion of serious and transnational crime, and magnified its impact.

Accordingly, the capacity to intercept content and/or capture related data from these communications is an essential law enforcement and anti-corruption method.

Organised crime threat picture

The 2011 ACC publication, *Organised Crime in Australia,* describes in detail the increasingly global scope of organised crime and the threat posed by international organised crime to Australia, as follows:

> **The contemporary face of organised crime**[2]
>
> Opportunities for organised crime today are unprecedented—increased globalisation, escalating cross-border movement of people, goods and money, emerging international markets and rapidly developing and converging technologies provide a fertile operating environment for organised crime.
>
> The picture of organised crime built up over the past decade reveals a dynamic, ever-evolving transnational phenomenon of immense size.
>
> Organised crime is sophisticated, resilient, highly diversified and pervasive. Current patterns of organised crime are more complex now than at any point in history.
>
> Organised crime groups are entrepreneurial and unrestrained by legislation, borders, morality or technology. They are adaptable, innovative and fluid—infiltrating a wide range of industries and markets, well beyond areas generally considered vulnerable.
>
> They are strategic and continually scan the marketplace for vulnerabilities, new opportunities and emerging technologies in order to make the greatest profit.
>
> They are flexible about changing direction to achieve their goals. They adjust operations in response to law enforcement efforts to harden the environment. They collaborate for mutual benefit and can quickly disperse and regenerate in other markets if disrupted.
>
> Organised crime operates within and alongside legitimate businesses, spanning multiple sectors to maximise return and minimise risk. Increasingly, organised crime uses logistics planning and aggressive marketing, buys in expertise and specialist facilitators and invests in research and development and risk mitigation strategies.
>
> Complex networks which engage in illicit transactions stretch across continents to support activities that range from drug importation to identity fraud, cybercrime to high level offshore tax evasion, counterfeit goods to money laundering and even environmental crime.
>
> To many, organised crime may seem like a distant threat, far removed from most people's lives. In reality, the social and economic harm that is caused through illicit drugs, financial crime and the associated violence and intimidation has a very real impact on the whole community.

[2] *Organised Crime in Australia 2011*, Introduction, p 3.

The law enforcement corruption context

In 2008–09, the Integrity Commissioner oriented ACLEI's strategic focus to corruption issues related to organised crime. This decision reflected a change in the threat picture, which was articulated in the then Prime Minister's *National Security Statement to the Parliament* in December 2008 and in the 2009 *Commonwealth Organised Crime Strategic Framework*.

The Organised Crime Strategic Framework recognises that the corrupt compromise of public officials and infiltration of government agencies are tactics used by organised crime groups to establish, further or conceal illicit enterprises and activities. Due to the sensitivity of their roles, public officials who work in law enforcement contexts present a particular corruption risk.

> RISK ONE: Familiarity with law enforcement techniques (and "inside knowledge" of their legal and technical limits) enables law enforcement officials to evade detection, and gives them confidence to act corruptly.

To highlight this change in the threat picture, and to explain in an engaging way the emerging risk, the Integrity Commissioner uses the term *'the corruption handshake'* to describe the potential relationship between corrupt law enforcement officials and organised crime. The term encapsulates the idea that, in most cases, corrupt conduct will involve a dishonest transaction between two parties which, to bystanders, may be invisible or appear normal.

> RISK TWO: Law enforcement officials provide information to criminal groups about law enforcement methods, to assist them to employ counter-measures and thereby evade detection. This knowledge creates a saleable commodity, places a corrupt official in the role of a facilitator of organised crime, and thereby frustrates or defeats legitimate law enforcement objectives.

"Match measures to risks"

ACLEI's jurisdiction and resourcing structure is founded on the concept of "matching measures to risks". Accordingly, since its commencement in 2007, ACLEI has developed in capacity, capability and scope to respond to emerging threats to integrity in Australian Government law enforcement environments. Some of these developments include:

- In January 2011, the Government extended the Integrity Commissioner's jurisdiction to include the Australian Customs and Border Protection Service.
- Earlier this year, the Minister for Home Affairs and Justice, the Hon. Jason Clare MP, announced the Government's intention to extend the jurisdiction further in 2013, to include the Biosecurity aspects of the Department of Agriculture, Fisheries and Forestry (the former Australian Quarantine and Inspection Service), the Australian Transaction Reports and Analysis Centre (AUSTRAC), and the CrimTrac Agency.
- The Minister has also announced the Government's intention to introduce legislation that will broaden the range of integrity testing that presently applies to staff members of prescribed law enforcement agencies.

These measures recognise both the seriousness of corruption and infiltration (if left unchecked), and the need to examine novel ways of combating organised crime.

Use of retained data in ACLEI operations

Anti-corruption investigations conducted by ACLEI are complex, and may involve multi-agency task-forces to achieve their objectives. Access to communications-related data and intercepted content is an essential part of investigations, since the information collected may provide direct evidence (which would be impractical to obtain in any other way) of the commission of serious criminal offences. Moreover, these methods can help to uncover complex corruption and serious crime that otherwise would remain hidden.

One pattern seen in organised crime and corruption is that central figures may use a range of contacts to contribute to a sequence of corrupt outcomes, such as facilitating the supply of illicit drugs. Under this "partition" model, several participants are used, either wittingly or unwittingly, to obtain access to and provide information, or to render other assistance to an illicit operation. Some contacts may be continually active, or be called upon only occasionally (to lessen suspicion and to retain their cooperation).

This "partition" model, now frequently used by organised crime, makes it difficult to know how wide a corrupt network may be, or how deep is the compromise. The "partition" model also may make it difficult to obtain evidence of offences sufficient to found a warrant application for telecommunications interception.

ACLEI uses network-analysis to build risk profiles in order to detect corrupt conduct. In appropriate circumstances, historical communications-related data (as opposed to intercepted content) may be used to establish patterns of corrupt activity by, for example, providing an indication of individuals' movements and associations. The same type of data also may be used to corroborate other information gathered during ACLEI investigations.

Accordingly, any proposal to formalise present arrangements for ancillary data to be retained by telecommunications carriers, in line with the Council of Europe protocols, would be an effective aid to investigate corrupt conduct.

Modernising existing arrangements

ACLEI is a "small user" of communications-based investigation methods. Even so, it is apparent from our experience that the present legislation is outmoded and no longer matches the ways in which criminals and corrupt officials use technology, including how counter-measures are used to defeat the capture of evidentiary material.

From ACLEI's perspective, there would be merit in moving towards a multi-purpose, single warrant system that:

- retains independent authorisation at the commencement of an interception operation, with provision for regular independent re-authorisation;
- is target- or issue-based, rather than technology-based;
- "matches measures to risks" and responds better to the organised crime "partition" model, for instance by adjusting the range of criminal penalty offences that establish the thresholds for warrant approval;
- is flexible, allowing investigators to respond to rapidly-changing operational circumstances, within set limits and in ways that provide for accountability after-the-fact (whether by post-inspection, or through the warrant re-authorisation process);
- simplifies procedures for sharing information across multi-agency task-forces and other similar arrangements, subject to appropriate safeguards; and
- updates accountability mechanisms to be privacy-focussed, rather than compliance-focussed, perhaps through closer alignment with the *Privacy Act 1988*.