Committee Secretary
Parliamentary Joint Committee on the Australian
Commission for Law Enforcement Integrity
PO Box 6100
Parliament House
CANBERRA ACT 2600

Dear Committee Secretary

Inquiry into Integrity Testing

The Office of the Australian Information Commissioner (OAIC) welcomes the opportunity to provide a submission to the Parliamentary Joint Committee on the Australian Commission for Law Enforcement Integrity Inquiry into Integrity Testing (the Inquiry).

The OAIC is established by the *Australian Information Commissioner Act 2010* (Cth) (AIC Act) and commenced operation on 1 November 2010. The former Office of the Privacy Commissioner (OPC) became part of the OAIC on this date. The OAIC is the national privacy regulator for personal information under the *Privacy Act 1988* (Cth) (Privacy Act). The OAIC has a similar regulatory role in relation to freedom of information under the *Freedom of Information Act 1982* (Cth) and a further role in relation to the Information Commissioner functions set out in the AIC Act, which comprise strategic functions relating to information management by the Australian Government.

Integrity Testing

The Inquiry will consider various integrity testing models, the legislative and administrative framework required to underpin an integrity testing regime, the Commonwealth agencies to which an integrity testing regime could apply, the potential role of the Australian Commission for Law Enforcement Integrity (ACLEI) in integrity testing, and any other relevant matters. As the OAIC understands it integrity testing will simulate opportunities for corrupt conduct in order to examine in a controlled situation the honesty of those individuals working within law enforcement agencies. It may involve the use of covert surveillance techniques and technologies which could increase the possibility that their personal information is collected, aggregated and distributed.

Privacy Act Coverage

The Privacy Act protects the personal information of individuals handled by Australian Government agencies and personal information held by all large private sector organisations, private health service providers and some small businesses. It does this through the application of binding privacy principles. It also applies in a modified form to Australian Capital Territory (ACT) Government agencies and to Norfolk Island government agencies.

The Information Privacy Principles (IPPs) contained in section 14 of the Privacy Act, regulate the collection, use and disclosure of personal information held by Australian and ACT agencies including those with law enforcement and regulatory functions. However, there are some exemptions to the application of the Privacy Act. The OAIC notes the application of the Privacy Act to ACLEI and those agencies currently subject to the Integrity Commissioner's jurisdiction varies and this may have implications for the consistency of privacy protection afforded to personal information handled as part of any integrity testing regime.[1]
The acts and practices of the Integrity Commissioner are exempt from the application of the Privacy Act.[2] Further, Australian Government agencies or organisations that engage in an act or practice related to a record that has originated with, or has been received from, the Integrity Commissioner or a staff member of ACLEI are also exempt from the operation of the Privacy Act.[3]

Of those agencies subject to the ACLEI's jurisdiction, the Australian Federal Police (AFP) and the Australian Customs and Border Protection Service (Customs and Border Protection) are subject to the Privacy Act. However, the acts and practices of the Australian Crime Commission (ACC) are exempt from the Privacy Act[4] as are acts and practices by Australian Government agencies or organisations related to a record that has originated with, or has been received from, the ACC or its Board.[5] The OAIC notes that although the ACC and ACLEI are not subject to the Privacy Act there are mechanisms in their enabling legislation which provide privacy protections.[6]

In 2008, the Australian Law Reform Commission (ALRC) released its Report 108: *For Your Information: Australian Privacy Law and Practice* (ALRC Report) following its review of Australia's privacy framework.[7] The ALRC in its Report considered that both the ACC and ACLEI were subject to separate systems of oversight and accountability which accommodated the tension between oversight requirements and the need to avoid disclosure of their sensitive operations. Further, the ALRC expressed the view that the Privacy Act may not be the appropriate mechanism to address privacy issues relating to the ACC and ACLEI.

The ALRC recommended that the ACC and the Integrity Commissioner, in consultation with the OPC, should each develop and publish information-handling guidelines. These

---

[1] The OAIC understands that the Integrity Commissioner's jurisdiction covers the Australian Crime Commission, the Australian Federal Police, the predecessor of the Australian Crime Commission – the former National Crime Authority, and the Australian Customs and Border Protection Service in respect of its law enforcement functions.
[2] Section 7(1)(a)(iiia) of the Privacy Act.
[3] Section 7(1)(ga) of the Privacy Act.
[4] Section 7(2) of the Privacy Act.
[5] Section 7(1)(f) of the Privacy Act.
[6] Section 51 of the *Australian Crimes Commission Act 2002* (Cth) prohibits ACC officials and staff from recording, communicating or divulging any information acquired by reason, or in the course, of the performance of their duties under this Act. Confidentiality requirements are imposed on the Integrity Commissioner and ACLEI staff through Part 13, Division 5 of the *Law Enforcement Integrity Commissioner Act 2006* (Cth).
[7] http://www.austlii.edu.au/au/other/alrc/publications/reports/108/.

information-handling guidelines should address the conditions to be imposed on the recipients of personal information disclosed by the ACC or ACLEI in relation to the further handling of that information.[8] The Australian Government has yet to respond to these recommendations.

Integrity testing and privacy protections

The OAIC recognises that the right to privacy is not absolute. It is necessary to balance privacy with other important social interests such as ensuring that law enforcement agencies do not engage in corrupt practices. This should not diminish the role played by privacy in democratic societies in according individuals the freedom to pursue their daily lives with respect, dignity and anonymity. The challenge is how to achieve an appropriate balance with the protection of important human rights and social interests that may sometimes intersect with privacy.

Generally, it is reasonable for individuals to expect that the privacy of their personal information will be respected, particularly where no suspicious or criminal activity is apparent. For this reason, while the OAIC recognises the important policy objective of ensuring that law enforcement agencies do not engage in corrupt practices, it is of the view that any integrity testing regime, particularly one which employs covert techniques and technologies, should build in mechanisms that will, to the greatest extent possible, protect an individual's personal information.

Adopting this approach will minimise the privacy risks to individuals and assist in preventing the unnecessary collection of personal information and any unauthorised uses or disclosures. Such mechanisms could also address the potential for fragmentation and gaps in privacy protections that may arise when personal information is handled across different jurisdictions and by entities that may not be covered by the Privacy Act. Further, establishing a robust privacy framework will help build community trust and confidence in how personal information is handled in the context of integrity testing. This may be regarded as particularly important given the potential capacity for integrity testing to intrude upon the personal life of those individuals working within law enforcement agencies.

To support the making of judgements about balancing the protection of privacy with other important public and social interests, the OPC developed a tool called the '4A framework' (see **Attachment A**). The 4A framework is intended to assist government agencies consider personal information handling issues in relation to new legislative measures, specifically relating to new law enforcement or national security powers. It is underpinned by the principle that measures that diminish privacy should only be undertaken where these measures are:

- necessary and proportional to address the immediate need, and
- subject to appropriate and ongoing accountability measures and review.

---

[8] See ALRC Recommendations 37-1 and 37-2.

The OAIC refers the Committee to the 4A framework. The OAIC suggests that the issues identified in the 4A framework may assist the Committee in assessing if any integrity testing models identified will only apply in circumstances where it is necessary and proportionate and that there are adequate privacy protections in place.

Yours sincerely

Timothy Pilgrim
Australian Privacy Commissioner

8 August 2011

Australian Government
Office of the Australian Information Commissioner

Privacy fact sheet 3

4A framework – A tool for assessing and implementing new law enforcement and national security powers

July 2011

The Office of the Australian Information Commissioner has developed a proposed framework for assessing and implementing new law enforcement and national security powers. The 4A framework sets out a lifecycle approach from development to implementation and review. The aim of the framework is to bring balance and perspective to the assessment of proposals for law enforcement or national security measures with significant effects on privacy.

Analysis

Careful analysis is needed in the development phase to ensure that the proposed measure is necessary, effective, proportional, the least privacy invasive option and consistent with community expectations. This analysis should involve consideration of the size, scope and likely longevity of the problem, as well as the range of possible solutions, including less privacy invasive alternatives. The impact on privacy of the proposed solution should be analysed and critical consideration given to whether the measure is proportional to the risk.

Authority

The authority by which the measure is implemented should be appropriate to its privacy implications. Where there is likely to be a significant impact on privacy, the power should be conferred expressly by statute subject to objective criteria. Generally, the authority to exercise intrusive powers should be dependent on special judicial authorisation. Intrusive activities should be authorised by an appropriately senior officer.

Accountability

Implementation of the measure should be transparent and ensure accountability. Accountability processes should include independent complaint handling, monitoring, independent audit, and reporting and oversight powers commensurate with the intrusiveness of the measures.

Appraisal

There should be periodic appraisal of the measure to assess costs and benefits. Measures that are no longer necessary should be removed and unintended or undesirable consequences rectified. Mechanisms to ensure such periodic review should be built into the development of the measure. This could involve a sunset clause or parliamentary review after a fixed period.

In summary:

Analysis – Is there a problem? Is the solution proportional to the problem? Is it the least privacy invasive solution to the problem? Is it in line with community expectations?

Authority – Under what circumstances will the organisation be able to exercise its powers and who will authorise their use?

Accountability – What are the safeguards? Who is auditing the system? How are complaints handled? Are the reporting mechanisms adequate? And how is the system working?

Appraisal – Are there built in review mechanisms? Has the measure delivered what it promised and at what cost and benefit?

For further information
telephone: 1300 363 992
email: enquiries@oaic.gov.au
write: GPO Box 5218, Sydney NSW 2001
GPO Box 2999, Canberra ACT 2601
or visit our website at **www.oaic.gov.au**