IGIS SUBMISSION TO THE AUSTRALIAN LAW REFORM COMMISSION REVIEW OF AUSTRALIAN PRIVACY LAW

I am writing to respond to two proposals contained in Australian Law Reform Commission (ALRC) Discussion Paper 72 which relate to my office.

I would make the general point that the Office of the Inspector-General of Intelligence and Security (OIGIS) has a niche role in Australia's accountability framework focusing on the application of relevant laws, principles and values to the intelligence agencies, which of necessity are treated separately from other areas of government.

One of the key drivers for the creation of OIGIS was that the general accountability mechanisms introduced in Australia in the 1970s and 1980s did not readily fit the activities of the intelligence agencies. Nonetheless, the importance of accountability and the appropriate adaption of administrative law and privacy principles to intelligence work, prompted the establishment of OIGIS.

I might also mention that the Australian Intelligence Community (AIC) has made a draft of its submission to this review available to me, but I do not propose to comment her in detail on either that submission or the proposals specific to the AIC agencies (proposals 31-1, 31-2, 31-3 and 31-4). However, I would emphasise that my office has a special role in respect of the six AIC agencies. I suggest that it is clear from the outline given in your Discussion Paper, that the current accountability arrangements are significant and effective. On that basis it is understandable that AIC agencies might question why there is any need for changes to existing structures.

In relation to proposal 31-5, I agree that while the nature of intelligence agencies means that much of the information pertaining to them is necessarily kept out of the public domain, making readily available the privacy rules and guidelines referred to in proposal 31-1 is appropriate. There are no significant security considerations and furthermore there is benefit in making available information about the ways in which the agencies are held to account.

The discussion paper proposes two specific changes to the requirements levied upon OIGIS in relation to privacy and the handling of personal information. I appreciate the opportunity to make comment on those proposals and will address each proposal in turn.

Proposal 31-6 The Privacy Act should be amended to apply to the Ispector-General of Intelligence and Security in respect of the administrative operations of that office.

In the discussion paper, the ALRC highlights that the exemption from the provisions of the *Privacy Act 1988* (the Privacy Act) is applied to the Australian intelligence agencies (as defined in the Privacy Act) in order to protect the sources, capabilities and methods of those agencies thereby ensuring their continued effectiveness.

It is appropriate that in situations where conventional transparency measures are not viable, that other arrangements are made. As the review indicates, the Australian intelligence agencies are subject to privacy requirements that are informed by the principles that underpin the Privacy Act. They are also subject to a robust accountability regime.

The remaining three agencies within Defence that make up the AIC are exempt from the operation of the Privacy Act in relation to their intelligence activities. However, the three Defence intelligence agencies are not exempt from the provisions of the Privacy Act where administrative records are concerned, such as those relating to employees. I understand that the Defence intelligence agencies do not regard this approach to be one that compromises their particular sources, capabilities and methods.

The ALRC proposal to amend the Privacy Act to apply to OIGIS in respect of its administrative operations, such as those relating to the handling of employee records is essentially a proposal to align OIGIS with the Defence intelligence agencies rather than remain aligned with the Australian intelligence agencies.

I think it most unlikely that subjecting OIGIS administrative records to the requirements of the Privacy Act would reduce the effectiveness of the agency or compromise national security. Hence I regard ALRC proposal 31-6 as both reasonable and practically achievable.

Proposal 31-7 The Inspector-General of Intelligence and Security, in conjunction with the Office of the Privacy Commissioner, should develop and publish information handling guidelines to ensure that the personal information handled by IGIS is protected adequately.

Currently, there are no OIGIS-specific handling guidelines for personal information along the lines outlined by proposal 31-7. However, OIGIS handles personal information in accordance with protocols and procedures that are entirely consistent with the policy objectives of the Privacy Act and necessarily closely aligned with those of the AIC. This alignment comes largely as a consequence of routine handling of the AIC's intelligence product and has the consequence of delivering strong protective measures for personal information managed by OIGIS.

There are three broad categories of personal information handled by this office:

1. Personal information relating OIGIS employees.

2. Personal information distributed to OIGIS in AIC intelligence product or otherwise accessed in the course of OIGIS work.

3. Person information provided to OIGIS by members of the Australian public.

Should proposal 31-6 be adopted, person information relevant to the administrative operations of the office would be subject to the information privacy principles of the Privacy Act and therefore OIGIS-specific handling guidelines for this category of personal information would be unnecessary.

The personal information distributed to or otherwise accessed by OIGIS in AIC intelligence material is an example of personal information that has originated with, or been received from an AIC agency and is therefore currently exempt from the requirements of the Privacy Act (in accordance with section 7(1)(f)). It would be inconsistent with the policy objective underlying that provision if OIGIS-specific handling guidelines for this category of personal information were required.

There is a nexus between this second category and the third which relates to personal information made available to, and stored by, OIGIS in relation to members of the Australian public. The intersection of the two categories occurs because this third category of personal information usually relates to complaints made by members of the Australian public about an AIC agency.

The protocols and procedures for management of personal information provided by members of the public to OIGIS reflect the existing framework set out in the *Inspector-General of Intelligence and Security Act 1986* (IGIS Act) the *Archives Act 1983* (the Archives Act) and the *Protective Security Manual* (PSM).

I would note also that information provided by the public in these situations occurs on an entirely voluntary basis. Additionally, the information is used only for the purpose for which it is provided. Generally this relates to the Inspector-General's inquiry functions set out in section 8 of the IGIS Act.

The voluntary provision of this category of information is important to note when considering privacy policy objectives about the accuracy of information. That information is up-to-date is bolstered by

section 11(2)(a) of the IGIS Act, which gives the Inspector-General a discretion to not inquire into complaints about events that occurred more than 12 months earlier.

There is a robust legislative regime applying to the protection by OIGIS of information, including intelligence information and person information. This is set out in section 34 of the IGIS Act.

I am particularly conscious of the impact an allegation or finding of misuse of information, including unauthorised disclosure, would have on this office. On that basis I manage closely the risks associated with this issue. I am pleased to say that in the 20 years since my office was established there has never been a credible or substantiated allegation of this kind made. I do not regard this good fortune, rather as a validation of the effectiveness of the existing protocols and procedures.

The IGIS Act also determines what information OIGIS can disclose in relation to inquiry findings and in the agency's annual report. Section 23 of the IGIS Act requires the Inspector-General to provide a written response to a complainant, where that complainant has been inquired into. This is to occur following confirmation from the relevant AIC agency that the response will not prejudice security, the defence of Australia or Australia's relations with other countries.

Similar requirements prevail in relation to the annual report. Section 35 of the IGIS Act makes provision for the Inspector-General to furnish the Prime Minister with an annual report and to table in each House of the Parliament those elements that will not prejudice security, the defence of Australia, Australia's relations with other countries or – as importantly – the privacy of individuals.

The policy alignment of OIGIS with AIC agencies in combination with the relevant enabling legislation provides a robust and reasonable protective framework for personal information handled and stored by OIGIS. The framework has been developed to meet the dual requirements of aligning to the policy principles that inform laws such as the Privacy Act while also ensuring that the security requirements of the AIC are maintained. Proposal 31-7 would not add protections to the existing frame work and on that basis I do not support it.

In closing I would like to say that regular reviews of Australia's privacy laws are welcome and important. The nature of the work undertaken by the AIC requires AIC and OIGIS staff to consider carefully privacy issues on a daily basis. The ALRC discussion paper is a useful contribution to that consideration. I would be pleased to contribute further to this review should you consider it useful.

6 December 2007