

24 April 2013

Ms Julie Dennett
Committee Secretary
Senate Standing Committee on Legal and Constitutional Affairs
PO Box 1600
Parliament House
Canberra ACT 2600

E-mail: legcon.sen@aph.gov.au

Dear Ms Dennett

I refer to your letter of 27 March 2013 inviting written submissions to the Committee's inquiry into the *Public Interest Disclosure Bill 2013* (the Bill).

Please find enclosed an ASIO-ASIS joint submission on the Bill for your consideration.

Should you have any further queries, please do not hesitate to contact us at [REDACTED]

Yours sincerely

[REDACTED]

(a) Director-General of Security
Australian Security Intelligence Organisation

[REDACTED]

Nick Warner AO
Director-General
Australian Secret Intelligence Service

ASIO and ASIS support the aims of the *Public Interest Disclosure Bill 2013* (the Bill) in seeking to¹:

- Promote the integrity and accountability of the Commonwealth public sector;
- Encourage and facilitate the making of public interest disclosures by public officials;
- Ensure that public officials who make public interest disclosures are supported and are protected from adverse consequences relating to the disclosures; and
- Ensure that disclosure by public officials are properly investigated and dealt with.

The Bill will enhance the accountability of public officials and protect the Government and Australian people against instances of wrongdoing or maladministration. It offers enhanced protections for whistleblowers making a public interest disclosure under the new scheme. ASIO and ASIS welcome the additional protections for whistleblowers, especially as they apply to those making a disclosure relating to intelligence officials or intelligence information.

The Bill recognises the current legislative framework governing the Australian Intelligence Community (AIC) by including AIC agencies within provisions relating to internal disclosures, and excluding AIC agencies from the provisions relating to public/ external disclosures. This importantly recognises the existing oversight and investigative powers of the Inspector-General of Intelligence and Security (the IGIS), an accountability mechanism which is external to ASIO and ASIS and underpins the trust Australians place in ASIO and ASIS's capacity to fulfil their functions effectively, and with propriety. The Bill also recognises the public interest in protecting intelligence information²; enabling a complaint or public interest disclosure to be properly investigated without risking damage to national security through publication of sensitive information.

Efficacy of the current regime

Section 26 of the Bill sets out the conditions under which disclosures can be made. The Bill makes clear that other than an internal disclosure³, no disclosure – whether an 'external' disclosure, 'emergency' disclosure or disclosure to a legal practitioner can contain intelligence information, as defined in section 41.

This exemption strikes a balance between accountability and protection of national security information. It explicitly recognises the current legislative and oversight framework in which intelligence officers and agencies are answerable to the IGIS. The IGIS is an independent statutory office holder and is completely separate from the AIC. The IGIS reviews the activities of the AIC agencies. The purpose of this review is to ensure that the agencies act legally and with propriety, comply with ministerial guidelines and directives and respect human rights. The IGIS conducts inquiries either self-initiated or at the request of government and may receive and can choose to investigate complaints about the actions of AIC agencies. The IGIS has broad powers of investigation including to require any person to answer questions and produce relevant documents, to take sworn evidence and unrestricted access to AIC agencies premises. Of specific relevance to the Bill is the efficacy of the broad powers of the IGIS in dealing with 'whistleblowing' by intelligence officers or other government employees in respect of intelligence information or intelligence agencies.

¹ See section 6 of the Bill, 'Objects'.

² Defined in section 41 of the Bill, 'Meaning of *intelligence information*'.

³ Defined in section 8 of the Bill.

Since 1 July 2004, the IGIS has received around 52⁴ separate complaints from AIC employees (current or ex-employees). The nature of the complaints vary, but all complaints examined by the IGIS are considered with a view to identifying any systemic issues requiring investigation including maladministration, inappropriate or illegal processes, procedures or actions. The remit of the IGIS extends to include individual employment issues, recruitment and vetting processes for ASIO and ASIS employees. The IGIS can also investigate matters raised by ex-AIC employees – this is particularly important because ongoing secrecy obligations can prevent a complainant from approaching other complaint handling bodies.

The IGIS has conducted two full investigations and eight preliminary investigations in respect of complaints originating with employees or ex-employees since 2004. The remaining complaints were resolved administratively (including those assessed as not being credible allegations or not within the responsibilities of the IGIS). Where the IGIS finds sufficient cause to investigate a complaint as an inquiry (and in particular when an inquiry results in criticism of an agency), the IGIS must consult with the agency head and responsible Minister. As the conclusion of such inquiries, the IGIS can recommend changes to rules or procedures, recommend an agency reconsider or change a decision, or pay compensation for any loss suffered by the complainant as a result of the agency's decisions or actions. While the Minister(s) and agency are not bound by the IGIS recommendations, the IGIS can choose to further report directly to the Prime Minister or Parliament in the event the response from the Minister or agency is unsatisfactory.

The IGIS releases an Annual Report, which is publicly available, setting out unclassified summary details of the inquiries undertaken and complaints received. Where a full inquiry has been undertaken, the IGIS may also seek approval from the responsible minister to release an unclassified version of the final report with recommendations (to allow the timely release of information to the public in advance of the next Annual Report being tabled in the Parliament). This is appropriate to ensure national security considerations are taken into account in disclosing any security sensitive information.

The IGIS provides an independent mechanism for concerns with the actions of AIC agencies to be raised and appropriately considered without the need for an external disclosure mechanism. This avoids the significant risks for national security, global intelligence relationships and the safety of individuals that any external disclosure mechanism would carry. The IGIS has ably provided the 'whistle blowing' function for ASIO and ASIS to date and will continue to do so with increased protections for those seeking to make a disclosure to that office under the regime to be introduced by the Bill.

The importance of a clear definition of 'intelligence information' to national security

Relevant legislation makes intelligence agency heads responsible for the classification and/ or releasability of intelligence information. In practical terms, this means agency heads bear an ongoing responsibility to protect:

- Sources of intelligence (which in some cases, can be a life/ death matter);
- Intelligence collection methods and capabilities (which again often present risks to personal safety of AIC officers or government officials);

⁴ Figure is drawn from summaries contained in IGIS Annual Reports from 1 July 2004 – 30 June 2012.

- Ongoing operations investigating threats to Australia and Australians; and
- Australia's relationships with foreign countries.

Under the Bill, no external disclosure may contain information concerning an intelligence agency or intelligence information. Proposed section 41 sets out the definition of intelligence information. The explanatory memorandum for the Bill states, in relation to section 41:

This section outlines what comprises intelligence information for the purposes of the scheme. This is also important in the context of section 26 which provides that external disclosure, emergency disclosures or disclosures to a legal practitioner ...will not be protected if they disclose of (sic) intelligence information. Intelligence information is treated in this way under the Bill because the disclosure of intelligence information can have grave consequences for Australia's national security, its relationship with other countries and the safety of individuals.

The definition in the proposed section 41 is supported by ASIO and ASIS as being clear and properly encompassing information requiring protection. Clarity is important because the onus of deciding whether the information is intelligence information lies with the discloser. The clarity of the definition of 'intelligence information' is critical to minimising the risk that intelligence information is released inappropriately under the scheme. Without a very clear definition of intelligence information, a person seeking to make a public interest disclosure may inadvertently release intelligence information. Such a release might put national security or personal safety at risk. For example if the name or identifying information of an intelligence source were released that person could be in personal danger and ASIO or ASIS's ability to further use that source would be compromised.

Additionally, prohibitions exist preventing the publication of the identities of ASIO and ASIS officers⁵. These prohibitions would prevent meaningful use of the Bill's provisions for a person seeking to make a complaint relating to or involving an ASIO or ASIS officer, except to the IGIS.

The disclosure of the identity of present or former ASIO or ASIS personnel may:

- Seriously compromise ongoing activities in which they are or were involved;
- Identify past operational activities;
- Warn targets that they were, or are, of security interest; and/ or
- Place these persons, their families and their property at risk of acts and threats of violence.

The importance of preserving this anonymity is highlighted by the fact that periodically attempts have been made to identify and photograph ASIO and ASIS officers. ASIO and ASIS officers have access to highly sensitive information, the unauthorised disclosure of which could cause significant damage to the security of Australia and other countries.

For a person seeking to make a public interest disclosure, the definition of 'intelligence information' will serve to guide a decision about whether, once certain information is disclosed, the discloser will be protected by the Bill. Additionally, the definition will guide consideration of whether a certain disclosure is likely to involve damage to national security or put lives at risk (as discussed above) through inappropriate disclosure of intelligence.

⁵ *Australian Security Intelligence Organisation Act 1979*, section 92; *Intelligence Services Act 2001*; section 41.

Preserving our global intelligence relationships

Australia has formal, legal agreements to protect classified information exchanged with certain countries. Some agreements are at treaty-level, others are diplomatic agreements such as an exchange of notes or a memorandum of understanding. For example, the *Agreement between the Government of Australia and the Government of the United States of America concerning Security Measures for the Reciprocal Protection of Classified Information* (25 June 2002⁶) sets out procedures and practices for the exchange and protection of classified information. Similar agreements have been established with a number of countries and are available publicly⁷.

Our allies expect the Australian Government to protect, absolutely, classified information supplied by them to the Australian Government. Foreign partner relationships rely on guarantees to protect intelligence information from disclosure, and would likely be seriously jeopardized should foreign partners consider ASIO or ASIS unable to uphold those guarantees. ASIO and ASIS depend upon the willingness of other intelligence services to share, confidentially, information, intelligence and technical capability to perform their functions. Without the ability to effectively perform its functions, ASIO for example would not be able to provide timely forewarning of threats to Australia's security and would be less able to take appropriate action to deal with those threats.

ASIO and ASIS support the Bill as currently drafted. The Bill recognizes the appropriateness and efficacy of the IGIS as a mechanism for whistle blowing complaints relating to ASIO or ASIS or intelligence information. Additionally, it ensures intelligence officers and intelligence information, including sources, methods and technologies, are appropriately protected. This scheme balances the interests of national security with the importance of openness and integrity in governance achieving a balance which accommodates both objectives.

⁶ [2002] ATS 25.

⁷ Australian Treaty Series, Department of Foreign Affairs and Trade (via the www.austlii.edu.au website).