Australian Government
Office of the Australian Information Commissioner

Committee Secretary
Parliamentary Joint Committee on Intelligence and Security
PO Box 6021
Parliament House
CANBERRA ACT 2600

Dear Committee Secretary

OAIC submission on the Inquiry into the National Security Legislation Amendment Bill 2014

The Office of the Australian Information Commissioner (OAIC) thanks the Joint Committee on Intelligence and Security (the Joint Committee) for the opportunity to comment on the *National Security Legislation Amendment Bill (No 1) 2014* (the Bill).

The OAIC welcomes the focus of the Inquiry on ensuring that the proposed measures to modernise and strengthen the legislative framework for the Australian Intelligence Community (AIC) are appropriately balanced by safeguards in the Bill, including safeguards to protect individuals' privacy. The OAIC also notes that the Statement of Compatibility with Human Rights (the Statement) that accompanies the Bill recognises the privacy impacts of the Bill and assesses the safeguards that will exist to address these impacts.

Office of the Australian Information Commissioner

The OAIC was established by the *Australian Information Commissioner Act 2010* and commenced operation on 1 November 2010. The OAIC is an independent statutory agency headed by the Australian Information Commissioner. The Information Commissioner is supported by two other statutory officers: the Freedom of Information Commissioner and the Privacy Commissioner.

The OAIC brings together the functions of information policy and independent oversight of privacy protection and freedom of information in one agency, to advance the development of consistent workable information policy across all Australian government agencies.

General Comments

The OAIC recognises the need for the AIC to have the powers necessary for it to perform its role in upholding Australia's national security. At the same time, the OAIC considers that it is important that any proposals to expand those powers are developed with a view to accommodating contemporary community expectations about the handling of personal information, as reflected in the *Privacy Act 1988* (Privacy Act) and guidance issued by the OAIC.

Australia's privacy laws recognise that the protection of individuals' privacy, through the protection of their personal information, cannot be an absolute right. Rather, those interests must be balanced with the broader interest of the community in ensuring that entities are able to carry out their functions and activities. However, where handling of individuals' personal information is authorised in the broader interests of the community (including upholding national security) it is important that those activities are accompanied by the appropriate level of privacy safeguards and transparency.

Ensuring appropriate transparency around the handling of personal information will allow people to understand (to the greatest extent possible) how the AIC handles their personal information, and for what purposes. Such transparency will help shape community expectations about the handling of personal information and engender increased community trust in the AIC.

In making these comments, the OAIC is mindful that the Privacy Act does not regulate the handling of personal information by the AIC. Rather, the Inspector-General of Intelligence and Security (IGIS) has oversight of the six AIC agencies, including the Australian Security and Intelligence Organisation (ASIO). Further, the OAIC recognises that the six agencies that make up the AIC are subject to written rules or guidelines that govern the handling of intelligence information, including personal information.[1] Specifically, ASIO is required to comply with guidelines issued by the Attorney-General under the *Australian Security Intelligence Organisation Act 1979* (ASIO Act) in the performance of its functions (Attorney-General's Guidelines). Those Guidelines require ASIO to consider the necessity and proportionality of handling personal information and, further, that any inquiries and investigations be undertaken using as little intrusion into individuals' privacy as is possible.

The OAIC understands that the current Attorney-General's Guidelines were last updated on 10 December 2007.[2] In view of the rapidly changing environment surrounding the data collection needs of the AIC, the community's continuing concern around how their personal information is handled and the need for transparency in those process and the substantial changes to the Privacy Act that took effect on 12 March 2014, the OAIC would welcome any review of the Attorney-General's Guidelines and be prepared to assist in any such review.[3] The OAIC suggests that this would help ensure that there is consistency across Australia's

---

[1] The OAIC understands that the ASIS, DSD and DIGO are required by the *Intelligence Services Act 2001* (IS Act) to make written rules regulating the communication and retention of intelligence information concerning Australian persons (see s 15 IS Act). Further, that the communication of intelligence information by DIO and ONA is governed by privacy guidelines, issued by the Minister for Defence in the case of DIO, and the Director-General of ONA in the case of ONA. For further information see www.igis.gov.au/.

[2] See ASIO, *ASIO Report to Parliament 2012-2013*, available at: http://www.asio.gov.au/img/files/ASIO-Report-to-Parliament-2012-13.pdf, p8.

[3] That the public expects high standards of transparency in the handling of their personal information is supported by the OAIC's 2013 *Community Attitudes to Privacy Survey*. The results of that survey revealed that nearly all Australians (96%) believe that government agencies should tell them how their personal information is handled; see OAIC *Community Attitudes to Privacy survey Research Report 2013*, available at: http://www.oaic.gov.au/privacy/privacy-resources/privacy-reports/oaic-community-attitudes-to-privacy-survey-research-report-2013.

privacy framework, and that the laws, rules and guidelines that make up that framework reflect contemporary community expectations about the handling of personal information. Further, consistent with the comments above, the OAIC suggests that a review might help to enhance community confidence in the safeguards and accountability measures in place.

Specific Comments

Co-operation with the private sector

The OAIC understands the Bill amends s 19(1) of the ASIO Act to clarify that ASIO is authorised to co-operate with the private sector, as the current lack of clarity is a concern for ASIO.

The OAIC appreciates that ASIO's ability to co-operate with the private sector is necessary to help protect Australia's critical infrastructure, which is often controlled by private sector entities. However, the OAIC considers that the scope of the activities captured by the term 'co-operate' and whether they involve the handling of personal information is unclear.

In that regard, the OAIC acknowledges the consideration of the privacy impacts of this amendment contained in the Statement, in particular, the confirmation that the Attorney-General's Guidelines would apply to any engagement between ASIO and the private sector. Further, the OAIC notes that the IGIS can inspect all records, and has oversight of the functions of ASIO, to ensure that it acts legally and complies with any ministerial directions and those Guidelines.

Building on those safeguards, the OAIC suggests that, to the greatest extent possible, additional clarity around the types of activities that fall within ASIO's power to co-operate with the private sector would improve transparency. This is particularly important where those activities involve the sharing of personal information between ASIO and the private sector, as the Privacy Act does not apply to personal information that has originated with, or has been received from an intelligence agency, including ASIO. The OAIC suggests that such clarity could be provided by including in the Explanatory Memorandum to the Bill additional explanation of the types of activities that are captured by the power to co-operate. This might assist the community to understand that, in certain circumstances, the AIC may handle types of personal information that individuals may not ordinarily expect, such as the content of communications.

Section 80P of the Privacy Act

Schedule 6 to the Bill creates two new offence provisions in the ASIO Act that relate to unauthorised dealing with, and recording of, intelligence information. Schedule 6 also updates the definition of 'designated secrecy provisions' for the purpose of the exemption contained in s 80P(2) of the Privacy Act.

Sub-section 80P(1) of the Privacy Act permits the collection, use and disclosure of personal information when an emergency declaration is in force and where certain conditions are satisfied. Sub-section 80P(2) then provides that an entity is not liable for contravening a

secrecy provision by using or disclosing personal information under subs 80(1) unless it is a designated secrecy provision in subs 80P(7).

The Bill amends the definition of a 'designated secrecy provision' in paragraph 80P(7)(a) and (c) of the Privacy Act by adding in the new offences created by the Bill. The Explanatory Memorandum to the Bill specifically considers these amendments, and notes that:

- the secrecy offences in the ASIO Act and the *Intelligence Services Act 2001* do not apply if a person has authorisation or approval from the relevant agency head (or another authorised person) to communicate information or deal with a record, and
- the ASIO Act makes express provision for the communication of information under Part VIA of the Privacy Act (see Explanatory Memorandum to the Bill, Para 887).

As the regulator responsible for the Privacy Act, the OAIC considers that these amendments appropriately balance the competing interests.

OAIC's 4A Framework

To further assist the Joint Committee's consideration of these issues, particularly with respect to balancing privacy interests with the broader interest of the community, the Joint Committee may find the approach contained in the OAIC's 4A Framework to be useful (a copy of the framework can be found in Appendix A).

Should the Joint Committee require any further information please contact Este Darin-Cooper, Director of Privacy Law and Practice

Yours sincerely

Timothy Pilgrim
Australian Privacy Commissioner

John McMillan
Australian Information Commissioner

4 August 2014

Appendix A

Privacy fact sheet 3: 4A framework — A tool for assessing and implementing new law enforcement and national security powers

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 life cycle 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?