

**UNCLASSIFIED**

**Parliamentary Joint Committee on Intelligence and Security**

**Inquiry into the National Security Legislation Amendment Bill (No. 1) 2014**

**Australian Security Intelligence Organisation's Submission**

**July 2014**

**Introduction**

The Australian Security Intelligence Organisation (ASIO) welcomes the opportunity to assist the Parliamentary Joint Committee on Intelligence and Security (PJCIS) in its inquiry as to whether the National Security Legislation Amendment Bill (No. 1) 2014 appropriately implements the recommendations agreed by the Committee in 2013 and its assessment of the balance of national security and safeguards proposed in the Bill. The Attorney-General's Department (AGD) has made a submission setting out the way in which the recommendations have been implemented. ASIO agrees with and supports AGD's submission.

This submission supplements the ASIO submission of 20 August 2012 and the subsequent ASIO evidence to the PJCIS in 2012/13 which set out ASIO's position with respect of the legislative changes that are now proposed in this Bill. The proposed legislative amendments fall into four broad themes (improved effectiveness, modernisation, cooperation and protection of information and capabilities). This submission addresses the safeguards that ensure ASIO is both ethical and accountable in what it does. ASIO strongly believes that the legislative amendments and associated safeguards (both existing and proposed) provide the right balance for Australia.

**ASIO's role and security intelligence**

ASIO's functions are set out in the *Australian Security Intelligence Organisation Act 1979* (ASIO Act) and include obtaining, correlating and evaluating intelligence relevant to security. In this context 'security' includes:

- a. the protection of, and of the people of, the Commonwealth and the States and Territories from:
  - i. espionage;

**UNCLASSIFIED**

- ii. sabotage;
  - iii. politically motivated violence;
  - iv. promotion of communal violence;
  - v. attacks on Australia's defence system; or
  - vi. acts of foreign interference;
- whether direct from, or committed within, Australia or not; and
- b. the protection of Australia's territorial and border integrity; and
  - c. the carrying out of Australia's responsibilities to any foreign country in relation to the matters mentioned above.

**The purpose of the Bill**

The Bill is intended to modernise and improve the legislative framework that governs the activities of the Australian Intelligence Community (AIC), primarily through changes to the ASIO Act and the *Intelligence Services Act 2001* (IS Act). This will better enable Australia's security, intelligence and law enforcement agencies to protect Australia and its interests from security threats.

The Bills amendments fall into four broad themes: effectiveness, modernisation, cooperation and protection of information and capabilities:

*Effectiveness*

- amendments to address issues being experienced with the scope and effectiveness of ASIO warrants include:
  - amendments to ASIO's computer access legislation (section 25A of the ASIO Act) to better reflect current and future technologies.
  - an ability to vary warrants and enable the Director-General to approve groups or classes of persons to exercise authority under a warrant, rather than the current need to name each individual who has authority.
  - introduction of an identified person warrant to allow ASIO to more quickly respond to rapidly developing and more serious threats.

**UNCLASSIFIED**

- clarifying that ASIO Act warrant powers which involve entry to premises include entry to or exiting a third party premises to execute a warrant.
- clarifying that the power to use the force (that is necessary and reasonable to do the things specified in a warrant) can be exercised at any time during the execution of the warrant, and includes (appropriate) use of force against a person.
- the introduction of a special intelligence operations (SIO) scheme similar to that available to law enforcement.

*Modernisation*

- modernising ASIO's surveillance device provisions to better align them with those available to police through the Surveillance Devices Act.
- modernising ASIO's employment provisions to better align with public sector arrangements.

*Cooperation*

- enabling ASIS to undertake an activity outside Australia for the specific purpose of producing intelligence on an Australian person (or class of Australian persons) without a Ministerial Authorisation, to support ASIO in the performance of ASIO's functions, at the specific request of the Director-General or a person authorised by the DG (except where ASIS reasonably believes that it is not practicable in the circumstances for ASIO to notify ASIS of its intelligence requirements on the relevant Australian or class of Australian persons), and only in relation to activities where ASIO would not require a warrant to undertake the same activities.
- clarifying the existing power for ASIO to cooperate with the private sector – for example, through our Business Liaison Unit, which aims to ensure that owners and operators of critical infrastructure and other members of the Australian business community can access timely declassified ASIO information on matters affecting the security of the assets and staff.

*Protection of information and capabilities*

- increasing the penalty for existing offences of unauthorised communication of

**UNCLASSIFIED**

national security information and introducing offences for unauthorised copying and/or removal of national security information for those working in, and with, Australia's security and intelligence community.

- enabling breaches of section 92 of the ASIO Act (publishing identity of an ASIO officer) to be referred to law enforcement for investigation when it is not otherwise relevant to security. Currently, ASIO can refer information that has come into the possession of ASIO in the course of performing its functions to the Police if the information relates to the commission, or intended commission, of a 'serious crime'. The ASIO Act defines a 'serious crime' as an offence punishable by imprisonment exceeding 12 months. As the offence of publishing the identity of an ASIO employee carries a penalty of imprisonment for one year, ASIO cannot communicate information to the Police merely in relation to the publication of the identity of an officer.
- introducing a prima facie evidentiary certificate regime to cover ASIO Act warrants, similar to the regimes in the *Telecommunications (Interception and Access) Act 1979* and the *Surveillance Devices Act 2004*. The regime seeks to protect the identity of ASIO officers, sources and sensitive capabilities, for the purposes of Court proceedings. The certificates will cover ASIO acts in connection with computer access or surveillance device warrants or in accordance with provisions allowing use of surveillance devices without warrants, and only in relation to the manner in which the evidence was obtained and by whom and not the evidence itself.

**ASIO's extensive oversight and accountability**

ASIO takes civil liberties and privacy seriously and supports the principles of accountability and oversight in relation to all national security legislation. ASIO believes that the range of existing safeguards provides an appropriate and effective framework of checks and balances in respect of ASIO's use of its powers and ensures that ASIO's activities are necessary and proportionate. ASIO accepts its responsibility to protect and keep confidential any personal information it may hold about Australians, including persons under investigation as well as persons assisting ASIO to carry out its statutory responsibilities. ASIO's methodology and operating procedures place an emphasis on the principle of "proportionality" and are designed to ensure an appropriate and proportionate response, having close regard to both individual privacy considerations and the potential gravity of the threat being investigated.

**UNCLASSIFIED**

The following framework ensures ASIO's activities are both appropriate and proportionate:

*External Oversight Mechanisms*

- ASIO's activities are subject to ongoing review by the Inspector General of Intelligence and Security (IGIS), who provides independent assurance regarding ASIO's adherence to the law and the propriety of ASIO's activities. When exercising the inquiry function, IGIS has significant powers, comparable to those of a royal commission, to obtain information, require persons to answer questions and produce documents, take sworn evidence and enter the premises of any intelligence or defence intelligence agencies. The IGIS provides an annual report to Parliament and regularly appears before the PJCIS;
- the Independent National Security Legislation Monitor reviews the operation, effectiveness and implications of Australia's counter-terrorism and national security legislation on an ongoing basis;
- ASIO provides an annual report to the Attorney-General and the Leader of the Opposition. The Attorney-General lays before the House of Parliament a version of the report which deletes matters which could prejudice security, international affairs and privacy of individuals;
- ASIO provides a classified annual report to the PJCIS in relation to its administration and expenditure;
- certain ASIO assessments can be appealed to the Administrative Appeals Tribunal and proceedings can be instituted against ASIO in the Courts; and
- the Attorney-General issues all ASIO warrants (which authorise more intrusive activities), other than questioning and questioning and detention warrants which are issued by a Judge appointed as an issuing authority under Part III, Division 3 of the ASIO Act. For every warrant authorised, ASIO must report to the Attorney General on the extent to which it assisted ASIO in carrying out its functions. The Attorney General's Department provides independent legal advice to the Attorney General regarding whether each proposed warrant meets the required legislative tests.

**UNCLASSIFIED**

*Internal Oversight Mechanisms*

- the Attorney-General's Guidelines issued under section 8A of the ASIO Act in the performance of its functions include requirements for ASIO's collection and handling of personal information and a requirement that investigations should be undertaken using as little intrusion into individual privacy as is possible, consistent with the performance of ASIO's functions;
- ASIO's methods for obtaining information must be proportionate to the gravity of the threat posed and the probability of its occurrence;
- ASIO has detailed authorisation processes for establishing an investigation; and as the level of intrusiveness of proposed investigative activity increases so does the seniority of ASIO officer required to authorise the activity. For many matters this requires approval by SES level senior managers;
- ASIO has comprehensive internal policies and procedures providing guidance to employees and ensuring that legal obligations are understood and complied with;
- ASIO is subject to specific legislative requirements and limitations including:
  - the Director-General has special responsibility under the ASIO Act to take all reasonable steps to ensure that the role of ASIO is limited to what is necessary for the purposes of discharging its functions; and
  - the ASIO Act does not limit the right of persons to engage in lawful advocacy, protest or dissent and makes clear that lawful advocacy, protest or dissent must not, of itself, be regarded as prejudicial to 'security' as defined in the ASIO Act.

These elements are designed to ensure a maximum degree of transparency, consistent with the requirements of national security.

ASIO would welcome the opportunity to provide any further information or clarification the Committee might need in making its deliberations.