# National Security Legislation Amendment Bill (No. 1) 2014 - amendments relevant to ASIS

## Amendments considered by the PJCIS 2013 Report of the Inquiry into Potential Reform of Australia's National Security Legislation

### 1 – Schedule 5 Item (new subparagraph 9(1A)(a)(iiia) of the *Intelligence Services Act 2001* - New Ministerial Authorisation Ground of operational security

This amendment implements Recommendation 38 of the PJCIS report.

The current Ministerial authorisation grounds in subparagraph 9(1A)(a) of the *Intelligence Services Act 2001* (ISA) do not specifically cover the situation where an Australian person is, or is likely to be, involved in activities that pose a risk, or are likely to pose a risk, to the operational security of ASIS. As a result, there are situations where ASIS is concerned about a threat to operational security involving an Australian person, but cannot seek ministerial authorisation to collect intelligence to properly assess that threat.

Operational security is about the protection of the integrity of ASIS operations from the risk of being undermined by foreign and non-State adversaries such as terrorist organisations, or reliance on inaccurate or false information. Operational security is part of ASIS's counter intelligence function under section 6(1)(c) of the ISA. It is important to the protection of individuals, maintaining the effectiveness of ASIS, as well as protecting Australia's international reputation.

The new ground is intended to address activities that pose a risk, or are likely to pose a risk to the operational security of ASIS but are not, or are not likely to be, a threat to 'security' (for example, espionage or sabotage or interference by foreign governments) as defined in the *Australian Security Intelligence Organisation Act 1979* (ASIO Act). The latter situation will continue to require the agreement of the Attorney-General in addition to Ministerial authorisation.

Given the different functions of the three agencies covered by the ISA, it only applies to the operational security of ASIS. However, the ability to seek a Ministerial authorisation on this ground is not restricted to ASIS, as it might be necessary for DSD or DIGO to produce intelligence to assist ASIS to properly assess the threat to its operational security.

***Safeguards and Oversight***

The existing safeguards under the Intelligence Services Act that currently apply to Ministerial authorisation grounds will equally apply to this new ground. In particular:

- Before issuing an authorisation under this new ground, the Minister responsible for the ISA agency must be satisfied of the factors in subsection 9(1) of the ISA:
    - that any activities which may be done in reliance on the authorisation will be necessary for the proper performance of a function of the agency
    - there are satisfactory arrangements in place to ensure that nothing will be done in reliance on the authorisation beyond what is necessary for the proper performance of a function of the agency; and
    - there are satisfactory arrangements in place to ensure that the nature and consequences of acts done in reliance on the authorisation will be reasonable, having regard for the purposes for which they are carried out.

- In accordance with paragraph 9(1A)(b) where the Australian person is also, or is also likely to be involved in a threat to security, the Minister responsible for the ISA will still be required to obtain the agreement of the Attorney-General before issuing an authorisation.

- Any intelligence produced may only be retained and communicated in accordance with the rules to protect the privacy of Australians made by the Minister under section 15 of the ISA

ASIS use of this new Ministerial authorisation ground remains subject to the oversight of the Inspector-General of Intelligence and Security (IGIS) who is responsible for assessing both the legality and the propriety of its use by ASIS.

**2 – Schedule 5 Item 11 – New Division 3 of Part 2 of the *Intelligence Services Act 2001*- activities undertaken in relation to ASIO**

This amendment implements the Government's response to Recommendation 39 of the PJCIS report. The report recommended that where ASIO and an ISA agency, such as ASIS, are engaged in a co-operative intelligence operation a common standard based on the standards prescribed in the ASIO Act should apply for the authorisation of intrusive activities involving the collection of intelligence on an Australian.

The Government has implemented the PJCIS's recommendation in part by enhancing ASIS's ability to cooperate with ASIO overseas by adopting the standards in the ASIO Act for ASIO's less intrusive activities in Australia. The purpose of this amendment is to better enable ASIS to assist ASIO overseas. While ASIS is primarily focused on foreign intelligence and ASIO is primarily focused on security intelligence the reality is that these functions will often intersect and overlap. It is in Australia's national interest that where this occurs Australia's foreign intelligence and security services are able to interact and work seamlessly together. It prevents unnecessary duplication of resources and important matters falling between the cracks.

Experience with the different legislative regimes applying to ASIS and ASIO has identified situations where ASIO could properly collect intelligence on an Australian person because it would be relevant to security, but ASIS cannot assist ASIO in collecting that intelligence. There are also situations where, even though ASIS can obtain an emergency ministerial authorisation under the current provisions of the ISA, the realities of operating in high threat areas mean that the opportunity to act quickly on the basis of that authorisation may have been lost.

The amendment addresses these issues by adopting a common standard based on the ASIO Act in respect of less intrusive activities, where ASIS and ASIO are co-operating in support of an ASIO function overseas. The amendment also addresses the existing risk with the current approval regime which may give rise to situations where ASIS could become aware of a serious threat to national security involving an Australian person, but it is not able to act quickly to seek further intelligence on that threat (for example, in the event of a possible terrorist attack)

This amendment will only apply to less intrusive activities overseas. That is, situations where ASIO would be able to produce intelligence on that Australian person in Australia without the need to obtain a warrant.

ASIS will still be required to obtain a Ministerial authorisation under section 9 of the ISA before undertaking particularly intrusive activities overseas (for example, the use of tracking devices, listening devices and the interception of telecommunications) or if its activities are unrelated to ASIO's requirements.

The agencies will continue to have distinct functions and comply with the other limits set out in their governing legislation.

***Safeguards and Oversight***

There are a range of appropriate safeguards, including:

- A requirement for a notice from ASIO (except in emergency situations where it is not practicable to obtain a notice);
- Retention of notices from ASIO and making them available for inspection by the IGIS on request;
- The notification of the IGIS and ASIO as soon as practicable when undertaking an activity in an emergency situation;
- ASIS will still be required to obtain a Ministerial authorisation under section 9 of the ISA before undertaking particularly intrusive activities overseas (for example, the use of tracking devices, listening devices and the interception of telecommunications);
- The Director-General of ASIS must ensure satisfactory arrangements are in place so that:
    - activities will be undertaken only for the specific purpose of supporting ASIO in the performance of its functions, and
    - the nature and consequences of acts done will be reasonable having regard to the purposes for which they are carried out;
- A requirement for the communication of intelligence to ASIO;
- A prohibition on communicating intelligence outside of ASIS without consultation with ASIO
- Annual reporting by ASIS to the Foreign Minister;
- The ability of the Foreign Minister and the Attorney-General to jointly issue written guidelines in relation to undertaking activities; and
- Any intelligence produced will only be retained and communicated in accordance with the rules to protect the privacy of Australians made by the Foreign Minister under section 15 of the Intelligence Services Act.

The conduct of each activity is subject the oversight of the IGIS who is responsible for assessing both the legality and the propriety of its use by ASIS.

**3 – Schedule 5 (Item 14) – new subclause 1(1A) of Schedule 2 of the *Intelligence Services Act 2001* - Participation in self-defence and weapons training**

This amendment implements Recommendation 40 of the PJCIS report.

ASIS staff members and agents have been permitted to carry weapons in dangerous locations overseas (like Afghanistan) since 2004. The carriage of weapons by ASIS is strictly for defensive purposes in accordance with Schedule 2 of the ISA.

Under the current regime, ASIS is only permitted to provide training in the use of weapons to ASIS staff members and agents. This appears inconsistent with ASIS's ability to use weapons to protect others who are cooperating with ASIS in the performance of its functions under section 13 of the ISA. At a practical level, this inconsistency restricts joint training exercises with close partners.

Such training is important as a lack of understanding poses a risk to ASIS staff members and to the persons whom ASIS is cooperating with.

***Safeguards and Oversight***

This amendment will only allow ASIS to cooperatively train with a limited number of Australian agencies that have a lawful right to carry weapons in Australia, such as the ADF and the AFP, as well as to train with a limited number of trusted foreign partners approved by the Foreign

Minister after consulting the Prime Minister and the Attorney-General . In practice, this will be US, UK, Canadian and NZ agencies.

The proposed amendment is not intended to allow ASIS to provide weapons, or training in the use of weapons, to ASIO officers.

In addition to meeting the requirements of section 13(1A), a further Ministerial approval for training of specified staff members of the relevant agency will be required in accordance with Schedule 2 of the ISA. Under paragraph 4 of Schedule 2 the approval must specify

> (a) the purpose for which the weapon or training is provided; and
> (b) any conditions that must be complied with in relation to the provision of the weapon or training; and
> (c) if the approval is for the provision of a weapon or training in the use of a weapon—the kind or class of weapon involved.

Schedule 2 also includes the requirement for all Ministerial approvals for the provision of training to be provided to the IGIS who oversees the legality and propriety of the operations of ASIS.

## Amendments not considered by the PJCIS in its 2013 Report

The following amendments, which were not considered by the PJCIS, either have arisen more recently (amendments 4 and 5) or have received increased priority given recent international high-profile events involving the unauthorised disclosure of sensitive information (amendment 6).

**4 – Schedule 5 Item 12 amendment to subsection 14(2) of the *Intelligence Services Act 2001* - The extension to the limited protection from liability for purposes that assist Intelligence Services Act agencies overseas**

An amendment is also proposed to the limited protection from liability in subsection 14(2) of the Intelligence Services Act to remove an anomaly in the application of the limited protection from liability from Australian criminal and civil laws.

Currently a person who assists an Intelligence Services Act agency inside Australia where the act is preparatory to, in support of, otherwise directly connected with the proper performance of the ISA agencies' functions receives the protection. However, they would not receive that protection if they happened to provide the same assistance outside Australia.

This is clearly anomalous and is not how the protection was intended to operate.

This amendment will ensure that people who assist the ISA agencies outside Australia are also provided with the same limited protection from Australian law where that act is preparatory to, in support of, or otherwise directly connected with the proper performance of the IS agencies' function. The people who are most likely to assist ASIS are officers from other Commonwealth agencies.

***Safeguards and Oversight***

The IGIS will continue to oversight the operation of section 14, and in any proceedings involving its operation, may certify any facts relevant to the question of whether an act was done in the proper performance of a function of an ISA agency.

**5 – Schedule 5 Item 16 – new subclause 1(2A) of Schedule 2 of the *Intelligence Services Act 2001* - Use of weapons and self defence techniques by ASIS staff members and agents in a controlled environment in limited circumstances.**

ASIS staff members and agents are currently restricted from using weapons in a controlled environment, where it would be lawful for any other Commonwealth officer and/or member of the public to engage in that activity and where the use would otherwise be consistent with the proper performance of an ASIS function.

For example, there are circumstances where it would be common for members of the public and other Commonwealth officers to engage in these activities overseas. if an ASIS staff member is unable to participate, it creates a potential distinction between them and others, which risks drawing undue attention to them and their activities. A controlled environment would include a gun, club, a firing range, or a martial arts club.

***Safeguards and Oversight***

The Guidelines issued by the Director-General of ASIS that are given to the IGIS will set out the limited circumstances in which this amendment will operate. This will include that only ASIS staff members who have received in appropriate familiarisation training would be able to engage in such activities.

The IGIS will continue to oversight ASIS's compliance with the guidelines, as well as the legality and propriety of ASIS activities, including use of weapons or self defence .techniques in a controlled environment.

**6 - Schedule 6- Protection of information**

The amendments in Schedule 6 will amend existing offence provisions in the ISA and ASIO Acts (applicable to ASIS, DSD, DIGO and ASIO respectively) and add new offences related to these intelligence organisations. It will also amend the ISA to apply all of these offences to the Office of National Assessment and the Defence Intelligence Organisation. In relation to ASIS the amendments will :

- increase the penalty from 2 years to 10 years imprisonment for the current offence provisions in section 39 of the ISA(which criminalises the unauthorised communication of certain ASIS information) and clarify that the offence applies to information acquired from another person; and

- insert new sections 40C and 40D creating new offences, punishable by a maximum of three years imprisonment, for unauthorised dealing or unauthorised recording of classified or sensitive national security information by an ASIS staff member or agent, or a person working under a contract, agreement or arrangement with or providing services to, ASIS. Unauthorised dealing includes where the person intentionally copies, transcribes, removes or retains classified or sensitive national security records without authority.

ASIS recognises the need for, and supports, these amendments.

***Safeguards and Oversight***

The offences in sections 40C and 40D include a specific defence in relation to information that has already been made publicly available with the authority of the Commonwealth. This defence has also been added to section 39.

A prosecution for one of these offences may only be instituted by the Attorney-General or with the Attorney-General's consent. A decision to prosecute also remains a matter for the Commonwealth Director of Public Prosecutions in the exercise of its independent prosecutorial discretion.

The offences do not displace the regime in the *Public interest Disclosure Act 2013* in relation to intelligence agencies and information. In particular, the secrecy offences will not apply to a disclosure to the relevant agency head or to the IGIS. Nor will the offences affect the requirement on a person to comply with a notice issued by the IGIS to produce documents or provide information.