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

Submission to the Parliamentary Joint Committee on Intelligence and Security

Dr Vivienne Thom
Inspector-General of Intelligence and Security

4 August 2014

Table of Contents

Executive summary

The changes proposed by the National Security Legislation Amendment Bill (No.1) 2014 (the Bill) are significant. This Inquiry by the Parliamentary Joint Committee on Intelligence and Security (the Committee) is examining whether the Bill appropriately implements recommendations agreed by the Committee in 2013 and seeks to assess the balance of national security and safeguards proposed in the Bill.

The Office of the Inspector-General of Intelligence and Security (OIGIS) provides an oversight regime that is a fundamental part of those safeguards. This submission focuses on arrangements for oversight of the proposed new powers for the Australian Security Intelligence Organisation (ASIO) and the Australian Secret Intelligence Organisation (ASIS).

The *Inspector-General of Intelligence and Security Act 1986* (the IGIS Act) provides sufficient authority to oversight these new powers, but the proposed amendments would increase the scope and complexity of oversight arrangements and the workload of the OIGIS. New powers proposed in the Bill that would require additional oversight include:

- Expansion of computer access warrants to cover systems and networks of computers and to allow disruption of computers. Oversight of these warrants will require sufficient expertise in the technical aspects of computer operations.

- Changes to surveillance device warrants to allow ASIO employees and ASIO affiliates to use surveillance devices without a warrant in a range of circumstances. There are no reporting requirements associated with such surveillance meaning oversight will be particularly important.

- Authorising ASIO to use force against persons; this requires oversight of training arrangements as well as investigation of any instances where force is used.

- A regime of identified person warrants that devolves some decision making from the Attorney-General to officials – whose decisions are subject to IGIS scrutiny.

- A scheme that allows ASIO to give its staff and other people immunity from Australian law. The scheme has limited reporting requirements and oversight will be required during the life of such operations, not only at their conclusion.

- Removing, in most cases, the requirement for ASIS to obtain ministerial authorisation before producing intelligence on an Australian person. This may be coupled with an increase in such activity.

- The creation of a category of people to be known as 'ASIO affiliates' who can be granted various powers under the ASIO Act. Identifying the boundaries of this class of people will be difficult in some cases.

The submission notes that where decisions are made by the Director-General of Security or agency staff rather than by the Minister, or where arrangements are streamlined, enhanced reporting and recordkeeping requirements could facilitate effective oversight without unduly increasing the administrative burden on the agencies. In particular, adding a requirement for ASIO to report on any use of force against a person, disruption of computers and access to third party property would assist oversight.

Background

Role of the Inspector-General of Intelligence and Security

The Inspector-General of Intelligence and Security (IGIS) is an independent statutory officer who reviews the activities of the Australian intelligence agencies:

- Australian Security Intelligence Organisation (ASIO)
- Australian Secret Intelligence Service (ASIS)
- Defence Signals Directorate, which the Bill would re-name Australian Signals Directorate (ASD)
- Defence Imagery and Geospatial Organisation, which the Bill would re-name Australian Geospatial-Intelligence Organisation (AGO)
- Defence Intelligence Organisation (DIO)
- Office of National Assessments (ONA).

The IGIS is currently supported by 11 staff. The Office of the IGIS is an agency for the purposes of the *Public Service Act 1999* and a non-corporate Commonwealth entity for the purpose of the *Public Governance, Performance and Accountability Act 2013.* The appropriation for the IGIS office in 2014–15 is $2.189m.

The Office of the IGIS is situated within the Prime Minister's portfolio. The IGIS is not subject to direction from the Prime Minister, or other ministers, on how responsibilities under the *Inspector-General of Intelligence and Security Act 1986* (the IGIS Act) should be carried out.

The IGIS Act provides the legal basis for the IGIS to conduct inspections of the intelligence agencies and to conduct inquiries of the Inspector-General's own motion or at the request of a Minister.

The overarching purpose of IGIS's activities is to ensure that each intelligence agency acts legally and with propriety, complies with ministerial guidelines and directives, and respects human rights. A significant proportion of the resources of the office has in the past been directed towards ongoing inspection and monitoring activities, so as to identify issues, including about the governance and control frameworks within agencies, before there is a need for major remedial action. At present OIGIS staff have access to all documents of the intelligence agencies and the IGIS is often proactively briefed about sensitive operations.

The inspection role of the IGIS is complemented by an inquiry function. In undertaking inquiries the IGIS has strong investigative powers, including the power to require any person to answer questions and produce relevant documents, take sworn evidence, and enter agency premises. IGIS inquiries are conducted in private because they almost invariably involve highly classified or sensitive information, and the methods by which it is collected. Conducting an inquiry is resource intensive but provides a rigorous way of examining a particular complaint or systemic matter within an agency.

The IGIS has a statutory role in providing expert evidence to the Administrative Appeals Tribunal and the Information Commissioner in disputed Archives and Freedom of Information matters. The IGIS also has a coordination and oversight role under the *Public Interest Disclosure Act 2013* (the PID Act) in relation to the intelligence agencies.

Schedule 1 – ASIO employment etc.

The Committee recommended modernising the provisions of the *Australian Security Intelligence Organisation Act 1979* (the ASIO Act) for secondments (recommendation 26) but made no other recommendations on ASIO employment-related matters. It noted that the proposals put to the Committee 'appear on their face to be of an innocuous administrative character'.[1]

ASIO affiliates

The Bill proposes to introduce the concept of 'ASIO affiliates' which has implications under the ASIO Act and for IGIS's oversight of ASIO.

The category of 'ASIO affiliates' is relevant to a number of substantive provisions in the Bill. For example:

- ASIO affiliates are to be subject to the rules about publication of their identity in s92 of the ASIO Act [2]and in the Public Interest Disclosure scheme.[3]
- ASIO affiliates are to be covered by secrecy provisions in the *Crimes Act 1914* by virtue of being deemed to be Commonwealth officers.[4]
- The proposed changes will enable the Director-General to appoint senior ASIO affiliates to make decisions in relation to ASIO warrants[5] including determining which persons are to be able to exercise the authority of a telecommunications interception warrant.[6]
- The provisions in the *Telecommunications (Interception and Access) Act 1979* (TIA) that allow ASIO employees to access telecommunications data held by carriers are to be amended to enable the Director-General or a Deputy Director-General to authorise ASIO affiliates to request such data for purposes connected to ASIO functions.[7]
- Proposed amendments to the TIA will enable ASIO affiliates, under an agreement or arrangement with ASIO, to undertake actions to discover if a listening device is being used, even if doing so entails interception of communications.[8]
- ASIO affiliates will be able to use a surveillance device without a warrant if they do so in accordance with an agreement or arrangement with ASIO.[9]
- Exceptions in the *Surveillance Devices Act 2004* and taxation legislation which currently only apply to ASIO employees are also to be extended to ASIO affiliates.[10]

The definition of an ASIO affiliate is also important for oversight purposes because the powers and functions of the IGIS are to be amended to cover ASIO affiliates (this is addressed below).

---

[1] Report of the Inquiry into Potential Reforms of Australia's National Security Legislation, May 2013, page 104
[2] See items 27–30 of Schedule 1 to the Bill
[3] See item 50 of Schedule 1, which amends the definition of intelligence information in s41 of the PID Act
[4] Item 26 of Schedule 1 of the Bill amends s91 of the ASIO Act to deem ASIO affiliates to be Commonwealth officers for the purpose of the *Crimes Act 1914*.
[5] See for example the proposed s24(3) of the ASIO Act to be inserted by item 8 of Schedule 2 to the Bill.
[6] Item 62 of Schedule 1 of the Bill
[7] See items 73–75 of Schedule 1 to the Bill
[8] Item 61 of Schedule 1 of the Bill amends the prohibition on interception of telecommunications in s7 of the TIA to allow affiliates (as well as ASIO employees) to do this. Also see item 69 of Schedule 1 in relation to stored communications.
[9] See proposed ss26C, 26D and 26F in item 29 of Schedule 2 to the Bill.
[10] See item 54 of Schedule 1 to the Bill in relation to exceptions to the prohibition on using, recording and communicating protected information under the *Surveillance Devices Act 2004* and item 55 of Schedule 2 to the Bill in relation to the exception to the prohibition on providing certain taxpayer information under *Taxation Administration Act 1953*

An ASIO affiliate is defined in item 4 of Schedule 1 of the Bill as follows:

> ***ASIO affiliate*** means a person performing functions or services for the Organisation in accordance with a contract, agreement or other arrangement, and includes a person engaged under section 85 and a person performing services under an agreement under section 87, but does not include the Director-General or an ASIO employee.

The definition clearly covers consultants and contractors engaged under proposed s85 and secondees under s87 of the ASIO Act. Such persons are readily identified and perform ASIO employee-like activities. However, the definition is broader and the boundaries are not always clear. The terms 'agreement' and 'arrangement' are particularly broad and individuals may not always even realise that they are ASIO affiliates. There is no requirement that the individual providing services or performing a function must be a party to the contract, agreement or arrangement with ASIO; they may for example be an employee of a party:

- If a cleaning company was engaged to clean the ASIO building, the staff of that cleaning company would be ASIO affiliates because they are performing services for ASIO in accordance with a contract, agreement or arrangement.
- The employees of a telecommunications carrier could be covered by the definition of an ASIO affiliate if they are involved in undertaking lawful interception activities or providing telecommunications data under an arrangement, agreement or contract between the carrier and ASIO.
- Staff of foreign government bodies would appear to be covered by the definition of an ASIO affiliate if they are performing functions or services for ASIO under some type of memorandum of understanding or similar arrangement.
- A person who provided information to ASIO in accordance with some sort of agreement or arrangement (written or unwritten) could be an ASIO affiliate.

There is no requirement for any central register of 'contracts agreements and arrangements' which would assist in determining who is an ASIO affiliate; indeed, such agreements and arrangements need not be in writing. As such it may not always be clear who falls within the class of an 'ASIO affiliate' for the purpose of oversighting the numerous legislative powers and restrictions that are dependent on the term.

ASIO secondments

> **Recommendation 26: The Committee recommends that the ASIO Act be amended to modernise the Act's provisions regarding secondment arrangements.**

Item 19 of Schedule 1 to the Bill would provide power for the Director-General of Security to arrange to second an individual to or from ASIO.[11]

When making a submission to the earlier Committee inquiry, I had understood that the secondment provisions contemplated in the original discussion paper related to secondments between Australian government agencies.[12] The proposed amendments make clear that a secondment arrangement can be agreed with any 'body or organisation (whether within or outside Australia)'. What is not entirely clear in the Bill is whether seconded officers will retain their ASIO powers while on secondment. The Bill appears not to address this issue, though the explanatory memorandum suggests that the policy

[11] Proposed s86 and 87 of the ASIO Act

[12] *Equipping Australia against emerging and evolving threats*, Attorney-General's Department, Discussion Paper, July 2012 pages 43–44 and IGIS submission to the PJCIS Inquiry into Potential Reforms of Australia's National Security Legislation, 23 August 2012, p16

intention is that the individual will only be able to exercise the powers of the 'gaining' agency.[13] From an oversight perspective it is important that it is clear what powers and functions individual has authority to exercise.

In the earlier submission I noted that:

> If the secondment proposal is adopted I would be looking to ensure that the changes are applied in such a way that it is clear to individual officers which agency they are undertaking an activity for and that 'secondments' are a true change in working arrangements for a reasonable period. In my view it would not be proper for such a mechanism to be used to circumvent limits placed on employees in other legislation. For example it would not be proper for an ASIS staff member to be 'seconded' to ASIO for a day or two to enable them to perform an activity that they would otherwise not be permitted to undertake.[14]

This remains my view. As the proposal is for secondments to be extended to allow secondments with private sector bodies and overseas organisations, oversight arrangements will need to be adapted to ensure that the IGIS office maintains awareness and oversight of the activities of ASIO employees wherever they are working.

IGIS Act changes

The proposed changes to the *Inspector-General of Intelligence and Security Act 1986* (the IGIS Act) were not addressed in the earlier Committee inquiry. The changes in items 42–48 of Schedule 1 of the Bill are incidental to the introduction of the new category of persons described as 'ASIO affiliates'. As noted above, there may be practical difficulties in identifying the boundaries of the class of persons who may be ASIO affiliates, but this will have to be addressed on a case by case basis.

The proposed amendments would enable the IGIS to look at matters relating to ASIO affiliates in a similar way to the current jurisdiction for ASIO employees.

[13] Explanatory memorandum to the National Security Legislation Amendment Bill (No.1) 2014 paragraph 68 (page 43)
[14] IGIS submission to PJCIS Inquiry into Potential Reforms of Australia's National Security Legislation, 23 August 2012, page 16

Schedule 2 – Powers of the Organisation

Definition of a computer

> **Recommendation 20: The Committee recommends that the definition of computer in the ASIO Act be amended by adding to the existing definition the words "and includes multiple computers operating in a network".**
>
> **The Committee further recommends that the warrant provisions of the ASIO Act be amended by stipulating that a warrant authorising access to a computer may extend to all computers at a nominated location and all computers directly associated with a nominated person in relation to a security matter of interest.**

The Committee commented that:

> 4.22 The Committee understands the desire of ASIO to enable warrants to extend to all computers located on a particular premises, or connected to a particular person; however it does not consider that the issue is appropriately addressed by amending the definition of "computer" but rather by amending the warrant provisions.

The current definition of a computer in s22 of the ASIO Act is:

> ***Computer*** means a computer, a computer system or part of a computer system

The proposed amendment would re-define a computer as follows:

> ***computer*** means all or part of:
> (a) one or more computers; or
> (b) one or more computer systems; or
> (c) one or more computer networks; or
> (d) any combination of the above.[15]

Computer system and computer network are not defined.

The explanatory memorandum describes this amendment as a 'clarifying' amendment:

> This amendment clarifies the ambiguity around the current definition of a computer in relation to a 'computer system' by extending the definition to 'computer networks' and by making it clear that the definition of 'computer' under the ASIO Act, means all, or part of, or any combination of, one or more computers, computer systems and computer networks.[16]

In the submission to the earlier Committee inquiry I noted that:

> … the term 'computers connected to a computer network' is potentially very broad in scope. It is difficult to contemplate when it would be reasonable to access *all* computers connected to a network in the absence of further limitations. Similarly 'computers on a particular premises' could inadvertently include computers that can have no connection whatsoever with the individual of interest. [17]

The related amendments in items 16 and 18 of Schedule 2 enable a single warrant to cover multiple computers including any computer on particular premises or any computer used by, or likely to be

[15] Item 4 of Schedule 2 to the Bill
[16] Explanatory memorandum to the National Security Legislation Amendment Bill (No.1) 2014, paragraph 230 (page 64)
[17] IGIS submission to PJCIS Inquiry into Potential Reforms of Australia's National Security Legislation, 23 August 2012, page 14

used by, a person (whose identity may or may not be known). The person or premises are to be listed in the warrant if the category of computers to be targeted is defined by a place or person.[18] Currently s25A(2) of the ASIO Act requires that the Minister have reasonable grounds for believing that ASIO access to data held in a *particular* computer (the target computer) will substantially assist in the collection of intelligence. Item 16 of Schedule 2 to the Bill will remove the word 'particular' from this requirement. As noted above, the terms 'computer' is also to be re-defined so that it also covers systems or networks of computers. Item 18 of Schedule 2 will make clear that the target computer can be a particular computer (as re-defined) or a computer (as re-defined) on particular premises or likely to be used by a particular person.

With the proposed definition of a computer, which can include one or more systems or networks of computers used by a particular person or on particular premises, the potential scope of computer access warrants is considerable. There is no obligation in the current or proposed legislation that would require ASIO at any point in time to actively consider whether information obtained under such a warrant is actually related to the individual who was the subject of the warrant and no obligation to promptly delete information generated by or about individuals who are not relevant to security.

The requirement in s31 of the ASIO Act, which applies to all ASIO warrants including computer warrants, is only that in circumstances where the Director-General has chosen to actively consider if a particular record is required for ASIO functions and is satisfied that it is not, then the record is to be destroyed. There is no obligation to undertake such a consideration. Consequently there is potential for a significant amount of information to be retained by ASIO about persons not relevant to security but who were the subject of, or created information on, a computer connected to a targeted network or system or that was on targeted premises.

Disruption of computers

Recommendation 21: The Committee recommends that the Government give further consideration to amending the warrant provisions in the *Australian Security Intelligence Organisation Act 1979* to enable the disruption of a target computer for the purposes of executing a computer access warrant but only to the extent of a demonstrated necessity. The Committee further recommends that the Government pay particular regard to the concerns raised by the Inspector-General of Intelligence and Security.

The Committee also commented that (references omitted):

> 4.33 The Committee notes the Attorney-General's Department's submission that there is a need to address difficulties that can arise in executing ASIO's computer access warrants. The Committee further notes that the ASIO Act should be amended so that the prohibition on disrupting computers does not apply to activities that would be necessary to execute the warrant.
>
> 4.34 The Committee also encourages the Government to consider including provisions in the ASIO Act that would prevent damage or cause loss to telecommunications systems operated by third parties.
>
> 4.35 The Committee agrees with the comments of the IGIS that this proposal should be framed carefully to minimise the impact on parties unrelated to the security matter:
>
> > As this proposal could directly affect the activities of persons unrelated to security interests it would be essential to have to clearly justify the case as to why it is appropriate to affect any lawful use of the computer. The reasons would need to balance the potential

[18] See proposed s25A(3A) in item 18 of Schedule 2 to the Bill

consequences of this interference to the individual(s) with the threat to security.

4.36 The Committee also agrees with the IGIS that there should be appropriate review and oversight mechanisms with particular attention to the effect of any disruption on third parties.

Currently the ASIO Act provides that warrants do not authorise ASIO to do anything that 'interferes with, interrupts or obstructs the lawful use of the target computer'.[19] The Committee was advised that this absolute rule causes practical problems for ASIO in executing warrants. The proposed changes in item 12 and item 25 of Schedule 2 do two things. First they raise the threshold for interference or loss from none to 'material' interference or loss. Second, they authorise material interference, interruption or obstruction where doing so is 'necessary' to do the things authorised by the warrant.[20]

The proposed provisions apply to both the targeted computer and third party computers.

From an oversight perspective the challenge for the IGIS will be in determining whether interference occurred and, if so, whether it was 'material' and 'necessary'. As is currently the case, it is unlikely that a person who experienced interference, interruption or obstruction would be aware that it was caused by an action of ASIO. The increasing complexity of computer related operations means that the IGIS office requires increased access to technical expertise to oversight these operations effectively.

A provision in the legislation that required ASIO to report on activities that interfere, interrupt or obstruct a computer in some way would assist oversight by highlighting cases where this has occurred. Specifically, it would assist oversight by the IGIS if the report to the Attorney-General on any warrant that authorised access to a computer was required to provide advice on the extent to which there was any interference, interruption, obstruction or loss or damage to a computer or a communication in transit that occurred as a result of actions under the warrant. The IGIS office routinely inspects a sample of warrant reports provided to the Attorney-General.

Access to third party computers

Recommendation 22: The Committee recommends that the Government amend the warrant provisions of the ASIO Act to allow ASIO to access third party computers and communications in transit to access a target computer under a computer access warrant, subject to appropriate safeguards and accountability mechanisms, and consistent with existing provisions under the TIA Act.

Item 23 of Schedule 2 to the Bill and related measures would enable ASIO to use a third party computer or a communication in transit where it was reasonable in all the circumstances to do so. The decision by an individual in ASIO on whether it was reasonable in all the circumstances to use the third party computer or the communication in transit would be open to scrutiny by the IGIS.

The proposed 'reasonable in all the circumstances' test is not the same as the test for a B-party warrant in the TIA. A B-Party warrant in the TIA is currently issued by the Attorney-General and is only available where the Attorney-General is satisfied that ASIO has 'exhausted all other practicable methods' or the interception 'would not otherwise be possible'.[21]

[19] ASIO Act s25(6) and s25A(5)
[20] Note that the same provisions relating to disruption of a computer also appear in the proposed identified persons warrant – see proposed 27D(7) and 27E(5) in item 41 of Schedule 2 to the Bill
[21] See s9(3) of the TIA

To assist IGIS in targeting inspection activity efficiently it would be beneficial if the report to the Attorney-General on the execution of the warrant was required to include advice on whether any third party computer or communication in transit was used, the reasons for such use, and the result.

Access to third party premises

> **Recommendation 35: The Committee recommends that the ASIO Act be amended to clarify that the incidental power in the search and computer access warrant provisions includes entry to a third party's premises for the purposes of executing those warrants. However, the Committee is of the view that whatever amendments are made to facilitate this power should acknowledge the exceptional nature and very limited circumstances in which the power should be exercised.**

Currently a computer access warrant issued under s25A of the ASIO Act can authorise access to *specified* premises. Item 19 of Schedule 2 to the Bill would change this to enable computer access warrants to allow those exercising a warrant to enter *any* premises for the purpose of gaining entry to or exiting the specified premises. The explanatory memorandum describes this as a 'clarifying' amendment and provides some examples of when this power might be used.[22] Each of the scenarios described in the explanatory memorandum may be reasonable but the words of the proposed amendment provide a much broader power; one that is not limited by necessity or unforseen or emergency situations.

The Bill proposes that third party entry also be authorised for search, surveillance device, foreign intelligence and identified person warrants.[23]

ASIO is required to adhere to the Guideline issued by the Attorney-General under s8A of the ASIO Act. Currently the Guidelines require that information is to be obtained using as little intrusion into individual privacy as is possible, consistent with the performance of ASIO's functions.

It would assist oversight if the report to the Attorney-General on all warrants was required to include advice on whether any third party premises were entered, the reasons for doing so, and the result of that access.

Surveillance devices

> **Recommendation 30: The Committee recommends that the ASIO Act be amended to modernise the warrant provisions to align the surveillance device provisions with the *Surveillance Devices Act 2004,* in particular by optical devices.**

The proposal that the Committee previously considered related largely to modernising the listening device warrant scheme to enable optical surveillance devices to be used separate to listening devices.[24] The changes in Schedule 2 of the Bill do this.[25] They also do significantly more.

Currently the surveillance devices provisions in the ASIO Act prevent ASIO from using surveillance devices without a warrant and then provide for a scheme of warrants. The proposed changes would remove the prohibition meaning that, in many cases, surveillance devices could be used without a warrant. A warrant would only be required where some other Commonwealth, State or Territory law prevented the use of the device (because for example it involved a trespass to property or was contrary to a State or Territory law that applied to ASIO). This appears to be broadly consistent with the structure of the *Surveillance Devices Act 2004.*

---

[22] Explanatory memorandum to the National Security Legislation Amendment Bill (No.1) 2014 paragraphs 270-273(pages 69-70)
[23] See items 10, 29, 39 and 41 of Schedule 2 to the Bill
[24] PJCIS Inquiry into Potential Reforms of Australian National Security Legislation, May 2013 p115–116
[25] See item 29 of Schedule 2 of the Bill

The proposed sections 26C, 26D and 26E of the ASIO Act provide express authority for ASIO employees and ASIO affiliates to use listening devices, optical surveillance devices and tracking devices without a warrant in certain specified circumstances (notwithstanding any other Commonwealth, State or Territory law).[26] This authority to use a surveillance device without a warrant is broadly consistent with the Surveillance Devices Act in relation to listening and optical devices (law enforcement officers require an authorisation to use a tracking device). The Surveillance Devices Act has detailed recordkeeping and reporting obligations that are absent from the proposed provisions for ASIO.[27]

The proposed changes would affect how the IGIS oversights the use of surveillance devices by ASIO. Currently the office is able easily to identify where the use of surveillance devices has been authorised by a warrant. The standard of ASIO warrant paperwork is high and IGIS staff look only at a sample of operations that involve warrants.

Under the proposed changes, the use of surveillance devices, particularly optical surveillance devices, may be without warrant in a wider range of cases – approval for their use will be internal to ASIO. To maintain effective oversight the IGIS will need to determine when a surveillance device has been used without a warrant, how it was authorised and whether the decision to authorise the use of the device was lawful and proportionate. Although it would assist in oversight if ASIO was required to report on the use of surveillance devices without a warrant, the risk of an unreasonable invasion of privacy might not justify this additional compliance cost.

The proposed provisions relating to the use of surveillance devices without warrant apply to use of the devices both by ASIO employees and also by ASIO affiliates acting in accordance with the contract, agreement or other arrangement. As noted earlier in this submission the class of people who may be 'ASIO affiliates' is potentially large and in some cases it may be difficult to identify who is, or is not, in the class. Where the agreement or arrangement is not a written one it may also be difficult to determine if the ASIO affiliate is acting in accordance with that agreement or arrangement when using a surveillance device. The proposed s26F of the ASIO Act is an 'opt-out' rather than an 'opt-in' provision such that all ASIO affiliates are potentially covered by the warrantless surveillance device powers unless they are specifically excluded by the Director-General or a delegate.

The proposed ASIO surveillance device warrants will automatically authorise access to third party premises for the purpose of gaining entry to the targeted premises.[28] In contrast, under the Surveillance Devices Act, law enforcement warrants only authorise access to third party premises if those premises are specified in the warrant and are adjoining or providing access to the premises.[29] My comments in relation to access to third party premises for computer warrants also apply to surveillance device warrants.

The proposed surveillance device warrants would also authorise the use of force against a person.[30] As noted below, if ASIO employees and ASIO affiliates are to be authorised to use force against a person a proper regime of training and oversight is required.

[26] See item 46 of Schedule 2 to the Bill which proposes a new s33(3) that deals expressly with other Commonwealth State and Territory laws
[27] See ss49–53 of the Surveillance Devices Act
[28] See proposed s26 in item 29 of Schedule 2 to the Bill, and also proposed 27F in item 41 of Schedule 2 in relation to the proposed identified persons warrants
[29] See s18(2)(a) of the *Surveillance Devices Act 2004*
[30] See proposed 26A(1)(c) of the ASIO Act in item 26 of Schedule 2 to the Bill

Exercise of authority under warrants

Recommendation 32: The Committee recommends that the ASIO Act be amended to establish classes of persons able to execute warrants

Item 8 of Schedule 2 to the Bill allows the Director-General of Security or an authorised senior ASIO employee or ASIO affiliate to empower a person or a class of persons to exercise the authority of a warrant.[31] ASIO will need to ensure that employees and other persons authorised to execute a warrant are properly trained and understand the limits of their authority under a warrant. If the Director-General or an ASIO employee or ASIO affiliate appointed to make authorisations appoints a large class of persons (for example by determining a class by level or work area), all ASIO employees, ASIO affiliates and other persons in that class would be required to have the appropriate training. This is essential where warrants authorise the use of force against a person.[32]

Search warrants – use of force against a person

Recommendation 36:The Committee recommends that the ASIO Act be amended to clarify that reasonable force can be used at any time for the purposes of executing the warrant, not just on entry, and may only be used against property and not persons.

The Committee specifically recommended against amendments that would enable ASIO to use force against a person. Item 14 of Schedule 2 amends the search warrant power to require that the warrant *must* authorise the use of any force *against persons and things* that is necessary and reasonable to do the things specified in the warrant. The explanatory memorandum describes this as a 'clarifying' amendment.[33] My view is that the ASIO Act does not currently authorise the use of force against persons in the exercise of a search warrant and that this would therefore be a new power.[34]

The proposed amendments will also authorise the use of force against a person in executing other warrants including computer, surveillance device and identified person warrants.[35]

The explanatory memorandum indicates that Federal Police or State or Territory police may accompany ASIO officers when executing a warrant. Police officers are trained in the use of force against persons.[36] Standard procedure in the Australian Federal Police when any use of force option is employed is to review those actions to ensure that they were appropriate and proportionate to the circumstances involved in the incident. If the intention is that ASIO employees and affiliates as well as police are to be authorised to use force against a person in connection with an ASIO warrant then they should be appropriately trained to do so. Proper oversight of the use of force against a person by ASIO employees and affiliates would require oversight of the training program as well as prompt reporting and review of any instance where an ASIO employee or ASIO affiliate used force against a person. This would not be required if the Bill provided for the use of force against a person only by police officers assisting ASIO in executing a warrant.

---

[31] Item 8 of Schedule 2

[32] See item 14 and item 27 of Schedule 2

[33] Explanatory memorandum to the National Security Legislation Amendment Bill (No.1) 2014 paragraph 263 (page 68)

[34] This is not to suggest that ASIO employees do not currently have the right of self-defence nor that police who may be assisting ASIO in executing a warrant are unable to utilise their normal police powers to, for example, intervene in an assault or to use force to arrest a person for a relevant offence such as the offences in Division 147 of the Criminal Code relating to threatening or causing harm to a Commonwealth public official or the offences in Division 149 relating to the obstruction of Commonwealth public officials.

[35] See proposed items 13-14, 27,29, 36 and 41 of Schedule 2 to the Bill

[36] Explanatory memorandum to the National Security Legislation Amendment Bill (No.1) 2014 paragraph 263 (page 68)

It would assist the oversight to require that the Attorney-General and the IGIS be notified as soon as possible if, in the execution of *any* ASIO warrant, force was used against a person.

Identified person warrants

> **Recommendation 24: Subject to the recommendation on renewal of warrants, the Committee recommends that the maximum duration of ASIO Act search warrants not be increased.**
>
> **Recommendation 29: The Committee recommends that should the Government proceed with amending the ASIO Act to establish a named person warrant, further consideration be given to the factors that would enable ASIO to request a single warrant specifying multiple powers against a single target. The thresholds, duration, accountability mechanisms and oversight arrangements for such warrants should not be lower than other existing ASIO warrants.**
>
> **Recommendation 31: The Committee recommends that the ASIO Act not be amended to enable person searches to be undertaken independently of a premises search.**

The proposed identified person warrants will enable the Attorney-General to give conditional approval to allow ASIO to use a range of specified powers against an identified individual. The Attorney-General or the Director-General of Security can then authorise the use of one or more of those powers for a period while the warrant is in force. The proposed changes do not grant ASIO the power to search a person other than in connection with a search of premises.

My earlier comments on the use of force against person, access to third party premises and the disruption of computers also apply to the proposed identified person warrants.

An identified person warrant can be in force for up to six months.[37] Authority for a search of premises can only be for up to 90 days,[38] but the Director-General can grant a further authority for a search of the premises during the life of a warrant so that, in effect, searches can be conducted for up to six months before the warrant needs to be renewed by the Attorney-General. Multiple searches can be authorised by the Director-General for multiple premises under a single identified person warrant.[39]

The introduction of identified person warrants will affect how the IGIS oversights warrants. Currently IGIS staff look at a sample of warrant submissions. Overall the standard of ASIO submissions to the Attorney-General seeking warrants is high. The IGIS does not have, and quite properly never has had, jurisdiction to review the judgment exercised by the Minister, though the IGIS can look at the case that ASIO has put forward. The new provisions will enable decision making to be devolved from the Attorney-General to the Director-General, whose decisions are subject to IGIS oversight. Many of the tests in the proposed legislation turn on whether the decision maker was satisfied on reasonable grounds that something will substantially assist in the collection of intelligence relevant to security. These decisions will be subject to IGIS oversight.

[37] See proposed 27C(4)
[38] See proposed 27J(5)
[39] See ss27J(3), (5) &(8)

Schedule 3 – Protection for special intelligence operations

Recommendation 28: The Committee recommends that the ASIO Act be amended to create an authorised intelligence operations scheme, subject to similar safeguards and accountability arrangements as apply to the Australian Federal Police controlled operations regime under the *Crimes Act 1914*.

As noted in my earlier submission, the ability to give its staff and other people immunity from Australian law would be a significant new power for ASIO.[40] Unlike the scheme that applies to police, the proposed scheme for ASIO has no external authorisation requirement, less likelihood of judicial scrutiny and no detailed reporting requirements.[41]

The proposed scheme places responsibility for authorising special intelligence operations on the Director-General and the Deputy Directors-General of ASIO. The Director-General or Deputy Director-General must be satisfied on reasonable grounds of the matters in proposed s35C of the ASIO Act including that the circumstances are such as to justify the conduct of a special intelligence operation. The reasonableness of decisions such as this by an official will be subject to IGIS oversight. Special intelligence operations may run for many years and periodic review during the life of the operation, not only at its conclusion, will be required. There is no obligation on the Director-General or a Deputy Director-General to cancel an operation if the grounds have ceased to exist or if they are no longer satisfied of the required matters.

The reporting obligations for special intelligence operations proposed by the Bill are limited to reporting on the extent to which the special intelligence operation has assisted ASIO in the performance of one or more of its special intelligence functions[42] and providing basic statistical information.[43] To enable effective oversight by the IGIS it will be essential that ASIO keep proper records of decisions and actions taken under the proposed scheme.

[40] IGIS submission to PJCIS Inquiry into Potential Reforms of Australia's National Security Legislation, page 17
[41] Proposed s35Q in item 3 of Schedule 3 to the Bill requires a report to the IGIS and the Attorney in the first 6 months and for the remainder of the period that authority has effect.
[42] Proposed s35Q in item 3 of Schedule 3 to the Bill
[43] Item 4 of Schedule 3 to the Bill requires annual reporting on the number of applications made and the number of authorisations given.

Schedule 4 – ASIO co-operation and information sharing

Co-operation with 'any other person or body'

Recommendation 33: The Committee recommends that the ASIO Act be amended to formalise ASIO's capacity to co-operate with private sector entities.

I have no concern with the principle that ASIO's ability to cooperate with private sector entities should be clarified. I am aware of the nature of the activities undertaken by the ASIO Business Liaison Unit and have not identified any concerns with its activities.[44] Nothing in the Bill limits the proposed extension of cooperation to the type of cooperation with private sector bodies undertaken by the Business Liaison Unit.

The proposed amendment in item 5 of Schedule 4 may be broader than what appears to be have been intended by recommendation 33. The proposed amendment would change s 19(1) of the ASIO Act to add a new paragraph to enable ASIO to cooperate with 'any person or body whether within or outside Australia'. This could include foreign bodies or persons not approved by the Attorney-General or a body that could not be approved as it did not have the characteristics of a 'foreign authority'. This could circumvent current authorisation and oversight arrangements that are in place to ensure compliance with human rights obligations.

[44] Paragraph 592 (p118) of the explanatory memorandum to the to the National Security Legislation Amendment Bill (No.1) 2014 gives the Business Liaison Unit activities as an example of cooperation.

Schedule 5 – Activities and functions of Intelligence Services Act 2001 agencies

New grounds for ministerial authorisation – operational security of ASIS

> **Recommendation 38: The Committee recommends that the *Intelligence Services Act 2001* be amended to add a new ministerial authorisation ground where the Minister is satisfied that a person is, or is likely to be, involved in intelligence or counter-intelligence activities in circumstances where such an investigation would not currently be within the operational authority of the agency concerned.**

While the wording of the proposed new grounds for a ministerial authorisation to produce intelligence on an Australian person is not the same as that suggested in recommendation 38, I understand that the 'mischief' to be addressed remains the same and that the difference in wording is as a result of refinements that occurred during the drafting process.

The proposed new grounds for a ministerial authorisation would enable the Minister to approve the production of intelligence on an Australian person if the Minister is satisfied that the 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'.[45] The expression 'operational security of ASIS' is defined in item 1 of Schedule 5 to the Bill as:

> ***operational security of ASIS*** means the protection of the integrity of operations undertaken by ASIS from:
>
> (a) interference by a foreign person or entity; or
>
> (b) reliance on inaccurate or false information.

There would seem to be significant overlap between this proposal and the existing grounds for authorisation relating to activities that 'are or are likely to be a threat to security' in s9(1A)(a)(iii) of the *Intelligence Services Act 2001* (ISA). For example, where the integrity of an ASIS operation is potentially undermined by actions of a terrorist organisation or the intelligence service of a foreign country this would generally fall within the existing security grounds. This of itself is not a problem from an oversight perspective as there are numerous circumstances where the facts of a particular case could fit into more than one category in s9(1A)(a). Section 9(1A)(b) makes clear that where there is an overlap with activities that are, or are likely to be, a threat to security the agreement of the Attorney-General is required in addition to authorisation from the agency Minister.

Removal of requirement for ministerial authorisation when ASIS is assisting ASIO

> **Recommendation 39: The Committee recommends that where ASIO and an ISA agency are engaged in a cooperative 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 person.**

Currently each of the foreign intelligence agencies (ASIS, ASD and AGO) requires prior approval from their Minister before undertaking any activity for the purpose of producing intelligence on an Australian person.[46] If the Australian person is, or is likely to be, involved in an activity or activities that are, or are likely to be, a threat to security (as defined in the ASIO Act) the agreement of the

[45] See item 6 of Schedule 5 to the Bill
[46] See s8 of the ISA

Attorney-General is also required.[47] These authorisations relate to specified individuals, not classes of individuals or categories of information.

The threshold that the agencies are currently required to meet to obtain a ministerial authorisation to produce intelligence on an Australian person for a security related matter is that the Australian person is, or is likely to be, involved in an activity that is, or is likely to be, a threat to security.[48] This is not a high threshold. The cases that are put to Ministers for authorisation generally go well above the relatively low threshold set by s9 of the ISA.

The fact that the foreign intelligence agencies require ministerial authorisation to undertake activities that ASIO can do without such authorisation also causes anomalies where the privacy rights afforded to an Australian depend to some extent on whether the Australian intelligence agency involved is ASIO or is ASIS, ASD or AGO.

The changes proposed by item 11 of Schedule 5 to the Bill will, in effect, remove the requirement for ASIS to obtain ministerial authorisation to collect intelligence on an Australian person in most cases. The proposed changes do not affect ASD or AGO. The changes do not place any obligation on ASIO to obtain ministerial authorisation for undertaking an activity overseas that would require a warrant in Australia. (ASIS will still require ministerial authorisation to undertake an action overseas for which ASIO would require a warrant in Australia.[49])

ASIS will be able to undertake activities outside Australia to collect intelligence on Australian persons to assist ASIO in the performance of any of its functions.[50] This activity may either be in response to a request from the Director-General of Security (or an SES equivalent level ASIO employee or ASIO affiliate authorised to make such requests) or the activity may be undertaken at the initiative of an authorised ASIS officer where they reasonably believe that it is not practicable in the circumstances for ASIO to notify ASIS of the requirement.[51] ASIS officers sometimes work in difficult environments and the reasons why it would not be practicable to contact ASIO first could relate to the timing of planned meetings with 'agents' and practical difficulties in accessing secure communications.

The legislation would not prevent requests from authorised ASIO employees or ASIO affiliates being cast in very broad terms or prevent ASIS authorising a broad category of staff to act on their own initiative when they reasonably believe that it is not practicable in the circumstances for ASIO to be contacted first.

ASIS will be required by the proposed s13F(2) of the ISA to communicate any intelligence produced under the new arrangements to ASIO. According to the explanatory memorandum the rules regulating the communication and retention of intelligence information concerning Australian persons that are made under s15 of the ISA will still apply.[52] The current rules made under s15 for ASIS allow the communication to ASIO of any intelligence that 'relates or appears to relate' to the performance of ASIO's functions.[53] It is difficult to envision any circumstance where this threshold will not be met in the context of the proposed new provisions. Any further communication of intelligence by ASIO would be regulated by the ASIO Act, noting that changes are proposed

[47] See s9(1A)(b) of the ISA
[48] See s9(1A)(a)(iii) of the ISA
[49] See proposed s13D of the ASIO Act in item 11 of Schedule 5 to the Bill
[50] ASIO's functions are listed in s17(1)(a)-(f) of the ASIO Act
[51] Proposed s13B and 13C of the ISA in item 11 of Schedule 5 to the Bill
[52] Explanatory memorandum to the National Security Legislation Amendment Bill (No.1) 2014 paragraph 647 (page 125)
[53] See Rule 3.3. The ASIS Privacy Rules are available on the ASIS website www.asis.gov.au

elsewhere in the Bill to expand the circumstances in which ASIO can disclose information and cooperate with other bodies (foreign and domestic).[54]

Currently ASIS produces intelligence on relatively few Australian persons. This number may increase with the changes proposed in the Bill. There is no requirement in the proposed provisions that would require ASIS to keep a register of Australian persons that are the subject of activity in response to an ASIO request under the new scheme.

The IGIS is to be notified when an ASIS officer produces intelligence on an Australian person in the belief that it is not practicable in the circumstances for ASIO to notify ASIS before undertaking the activity; this requirement will assist in oversight of such activity.[55]

IGIS oversight of the production of intelligence on Australian persons by ASIS to meet ASIO requirements will continue, although it will be more complex.

Weapons training

Recommendation 40: The Committee recommends that the ISA be amended to enable ASIS to provide training in self-defence and the use of weapons to a person cooperating with ASIS.

Items 14–15 and 17–20 of Schedule 5 to the Bill would allow ASIS to provide weapons and training in weapons and self-defence to individuals from other agencies who are cooperating with ASIS. Oversight of the training of individuals from other agencies could be undertaken as part of routine inspection by OIGIS staff of ASIS weapons and self-defence training programs.

Item 16 of Schedule 5 to the Bill provides authority to use weapons in 'a controlled environment'. This is described in the explanatory memorandum as a 'clarification' but, in my view, is a new power.[56] In late 2013 I completed an inquiry into the provision of weapons and the training in and use of weapons and self-defence techniques by the ASIS.[57] In that report I noted that 'Since 2004 there have been two breaches of the ISA, both involving the discharge of a firearm without appropriate prior approval. Both incidents occurred within controlled weapons training environments and were not indicative of systemic issues.' Incidents of this nature would not be reported as breaches if the legislation is amended as proposed.

[54] See for example cooperation under item 5 of Schedule 4 and secondments under items 86 and 87 of Schedule 1
[55] See proposed 13B(4) of the ISA
[56] Explanatory memorandum to the National Security Legislation Amendment Bill (No.1) 2014 paragraph 664 (page 127)
[57] A summary of this inquiry is available at www.igis.gov.au

Schedule 6 – Protection of information

My comments on changes to secrecy provisions are limited to any potential impact they may have on the work of the IGIS office. Complainants to the IGIS, particularly those who have worked in the intelligence community or have entered into some contract, agreement or arrangement with an intelligence agency, require clear advice about whether secrecy laws or undertakings prevent them giving information to the IGIS when making complaints or proactively disclosing matters to the office. (There is no lack of clarity during the conduct of an inquiry where information is provided in response to a formal notice; however, most information used by the IGIS is obtained by IGIS staff during routine inspections, not using formal inquiry powers and not as a result of disclosures by 'public officials' under the PID scheme.)

While the heads of each intelligence agency have indicated that it is not their intention to limit the disclosure of information to the IGIS or IGIS staff and that, if requested, they would authorise any such disclosure, it is not satisfactory for complainants, disclosers or IGIS staff to rely on such express or implied agreement. There should be clear statutory authority for individuals to provide information to the IGIS for the purpose of complaints and inspections under the IGIS Act, notwithstanding other laws, agreements or undertakings.

In addition, OIGIS staff are sometimes required by an agency to sign an agreement before they access agency information. The broad definition of an 'entrusted person' in the proposed s18A(5) means that IGIS staff may inadvertently be subject to this secrecy provision in relation to information they acquire when inspecting agency records.[58] Similarly, some provisions such as the proposed 35P in relation to information about special intelligence operations appear absolute in their terms.[59] There is no difficulty with restricting public disclosure of information by IGIS staff, the IGIS Act does this, but there should be no doubt that information that IGIS staff identify during inspection activity can be conveyed to the IGIS and to other IGIS staff in the course of their duties.

[58] See item 4 of Schedule 6 to the Bill
[59] See item 3 of Schedule 3 to the Bill