School of Law
University of New England
Armidale NSW 2351
Australia

Associate Professor Greg Carne

The Committee Secretary
Parliamentary Joint Committee on Intelligence and Security
Parliament House
Canberra ACT 2600

5 August 2014

Re: Submission to Inquiry into the National Security Legislation Amendment Bill (No 1) 2014

Thank you for the opportunity to provide a submission to the Parliamentary Joint Committee on Intelligence and Security Inquiry into the *National Security Legislation Amendment Bill* (No 1) 2014.

This submission focuses on the legislative amendments proposed in Schedule 2 (Powers of ASIO), Schedule 5 (Activities and Functions of Intelligence Services Act 2001 agencies) and Schedule 6 (Protection of Information of Intelligence Agencies)

General overview of the Bill

The purpose of the PJCIS inquiry is advised as scrutinising "whether the Bill appropriately implements recommendations agreed by the Committee last year and to assess the balance of national security and safeguards proposed in the bill". As a preliminary to addressing this question in examining Schedule 2, Schedule 5 and Schedule 6 of the Bill, some general observations about the context and circumstances of the Bill can be usefully made.

The Bill is characterised by expansions of executive discretion and executive delegation of authorisation procedures and co-operative procedures, with a general expansion of intelligence agency powers in several areas. These matters appear to have been advocated in both the Discussion Paper *Equipping Australia Against Emerging and Evolving Threats* and in the Explanatory Memorandum to the Bill on grounds of efficiency, which may in part be a consequence of an ever growing scope of intelligence agency powers, but perhaps also on some unstated principle of agency convenience.

Parallel to this expansion of powers is a questionable approach to safeguards, which do not appear on close scrutiny to adequately check and balance the proposed powers. Of particular note is a weakening of existing safeguards (around Ministerial warrants, delegations of decision making power and ministerial authorisations) and an over-reliance upon the operational reasonableness and proprieties of the Director General in relation, for example, to the substantive exercise of authority under an identified person warrant, in authorising various delegations of decision making authority to senior ASIO office holders and in ensuring that satisfactory arrangements exist in relation to activities undertaken by ASIS in relation to ASIO.

A similar modelling of an increase in intelligence agency powers on criminal investigatory principles (for instance, third party interception warrants in relation to computer access and controlled operations schemes) does not necessarily translate successfully to a national security and intelligence agency environment, because of an enhanced need for secrecy and lack of openness in the review and monitoring of intelligence agency practices.

Of further moment in relation to the expanded intelligence gathering capabilities and streamlined co-operative arrangements in the present Bill is that these practices and the quantum of intelligence generated potentially have larger exponential consequences. This is because these expanded capacities will in turn feed into the generalisation of ASIO intelligence sharing and co-operative assistance introduced in 2011 for intelligence, law enforcement and federal and state government functions by the *Telecommunications Interception and Intelligence Services Legislation Amendment Act 2011* (Cth) and the *Intelligence Services Legislation Amendment Act 2011* (Cth)

Importantly, the signature characteristic of the Bill's conferral of executive discretions and executive delegations *sited below* the traditional requirements of Ministerial warrant or other Ministerial authorisation in the *ASIO Act 1979* (Cth) and the *Intelligence Services Act 2001* (Cth) (as an important and practical application of the doctrine of ministerial responsibility) means that a significantly heavier reliance now accrues for the accountability standards that may operate through the offices and powers of the Inspector General of Intelligence and Security and the Independent National Security Legislation Monitor.

In this respect, the latter office has only recently been reprieved from its abolition envisaged in the *Independent National Security Legislation Monitor Repeal Bill 2014* (Cth), and was a part time position with one full time office staff member. It appointment, follow up to past recommendations and its future priorities remain unclear. The Bill also institutes a greater legislated role for the Inspector General of Intelligence and Security,[1] whilst the role of the Inspector General of Intelligence and Security in relation to the amendments in the Bill is cited as important safeguards.[2]

---

[1] See for example, proposed amendments: s.35Q *ASIO Act 1979* (Cth) (regarding special intelligence operations); s.13B (3) of the *Intelligence Services Act 2001* (Cth) in relation to the obligation on ASIS to report ASIS self-activated activity in support of ASIO without a prior written request from ASIO.

[2] The Parliamentary Statement of Compatibility with Human Rights (in accordance with Part 3 of the *Human Rights (Parliamentary Scrutiny) Act 2011* for the Bill also raises the safeguard of the "independent oversight role of the Inspector-General of Intelligence and Security" in relation to the Schedule 2 warrant powers amendments (Page 11), the Schedule 3 Protection for Special Intelligence Operations (Page 17), the Schedule 4 co-operation and information sharing arrangements (Page 25) and the Schedule 5 Activities and functions of Intelligence Services Act 2001 agencies (Pages 27 and 28)

Given that the trend in this legislation is to incremental enlargement of intelligence agency powers and discretions, the Bill comprehensively fails to address financing and resourcing issues for the important oversight mechanisms of the Independent National Security Legislation Monitor and the Inspector General of Intelligence and Security.

It is timely that a comprehensive audit of these supervisory and monitoring riles is made, with a view to fixing in legislation a minimum budgetary allocation for the Inspector General of Intelligence and Security and the Independent National Security Legislation Monitor, representing a mathematical proportion of the overall budgetary appropriation to the members of Australia's intelligence community.

It is important in assessing the Bill's content in relation to safeguards and accountability, that the primary obligation of national security is the protection of a democratic society:

> Our national security interests must also be pursued in an accountable way, which meets the Government's responsibility to protect Australia, its people and its interests while preserving our civil liberties and the rule of law. This balance represents a continuing challenge of all modern democracies seeking to prepare for the complex national security challenges of the future. It is a balance that must remain a conscious part of the national security policy process. We must not silently allow any incremental erosion of our fundamental freedoms[3]

I will now proceed to an analysis of the balance of national security and safeguards proposed in the Bill in relation to Schedules 2, 5 and 6.

[3] First National Security Statement to Parliament 4 December 2008

Schedule 2: Powers of the Organisation

In considering under Schedule Two the question whether the Bill "appropriately implements the recommendations agreed by the Committee …and to assess the balance of national security and safeguards proposed in the Bill", it is important to highlight some distinctive conceptual shifts within the Schedule which weaken existing accountability measures and liberalise surveillance capabilities.

. Removal of general prohibition on ASIO use of certain devices

The starting point is the removal of the "general prohibition on ASIO's use of listening devices, tracking devices and optical surveillance devices and [identification of] the circumstances under which ASIO can use a surveillance device without a warrant".[4]

The existing legislation is based on principles of *restriction and exceptionality* in the use of such devices and in the interception of postal service and delivery service articles – through common statements of the unlawfulness of such activity, unless their use is authorised by a warrant under prescribed conditions by the Attorney General.

In contrast, the Bill proposes an *expanded and more permissive* surveillance regime including both warrant based and warrantless applications of listening devices, optical surveillance devices and tracking devices, stating that 'the use of surveillance devices is primarily regulated by State and Territory law [and] any use of a surveillance device by ASIO outside this framework will, generally, be regulated by State and Territory law". [5] As the Bill is thus configured, it may well contemplate the use of a surveillance device by ASIO, for example, under the co-operative arrangements instituted in the 2011 legislative amendments to the ASIO Act.

Whilst the test for the issue of a warrant based authorisation for the use of a surveillance device in the Bill has been adopted from the standard in the existing legislation, [6] the bill loosens accountability standards in several ways.

First, the important qualifier that "It is the duty of the Director-General to take all reasonable steps to ensure that this subsection is not contravened[7]" is removed from the legislation, without explanation.

Second, the use of an optical surveillance device without a warrant is broadly cast ie "may install, use or maintain an optical surveillance device without warrant if the installation, use or maintenance of the device does not involve (c) entering premises without permission from the owner or occupier of the premises"[8] – for example, thus permitting apparently reverse use of a computer web cam and loudspeakers, or the use of an aerial surveillance drone for legislated purposes, without a warrant.

---

[4] Explanatory memorandum to Bill 73.
[5] Explanatory memorandum to Bill, 73
[6] *ASIO Act 1979* (Cth) eg S.26, 26B, 26C, 27 (2) (a) and (b), 27 AA (3)(a) and (b)(that the Minister is satisfied that) (a) the person is engaged in, or is reasonably suspected by the Director General of being engaged in, or of being likely to engage in, activities prejudicial to security and (b) the use by the Organisation of …will, or is likely to, assist the Organisation in carrying out is function of obtaining intelligence relevant to security
[7] See Eg ASIO Act 1979 (Cth) s.26(1) (c), s.26A(1)
[8] Proposed s.26 D of the *ASIO Act 1979* (Cth)

Third, the collapsing of the separate identified surveillance devices as defined in the proposed Section 22 definition [9] into a single warrant that may be issued in relation to one or more of a particular person, particular premises or an object or class of object and in respect of more than one kind of surveillance device [10] *is likely to produce maximised applications for the use of warrant powers in a single warrant* in both (a) the range of surveillance devices and (b) collectively applying in relation to persons, premises and objects.

There is nothing (over and above the basic test for the issue of a surveillance device warrant in s.26 (3)(a), (b) and (c) of the Bill) to reinforce tests of necessity and proportionality in both the extent and range of surveillance devices (ie the number of methods of surveillance) and in relation to their cumulative application to persons, premises and objects.

. Introduction of identified person warrants

In the Bill's introduction of identified person warrants with its system of conditional approval to exercise one or more of the broad types of warrant powers in Division 2 of Part III which are specified in the warrant, it is claimed that "In fact, the test for an identified person warrant is more stringent than the various tests that currently apply to the issuing of warrants authorising ASIO to do comparable things under Division 2 of Part III".[11]

This statement is misleading, as the conditional approval scheme actually liberalises and devolves important warrant related matters from the Minister to the Director General, matters which formerly would have been subject to approval in the warrant itself by the Attorney General, who is the politically accountable figure for ASIO warrant operations under a system of ministerial responsibility and responsible government. That level of political accountability is clearly truncated by the Bill's warrant arrangements.

The PJCIS Report recommended that [t]he thresholds, duration, accountability mechanisms and oversight arrangements for [identified person] warrants should not be lower than other existing ASIO warrants.[12] The Bill's test for the issue of a warrant carries over the existing criteria for which the Minister must be satisfied,[13] but now gives conditional approval, in the most general descriptive terms, for ASIO to do one or more of a range of things.[14]

Subsequent authorisation to act under a identified person warrant covers a range of topic matters – search of premises and persons, computer access, surveillance devices, inspection of postal articles and inspection of delivery service articles – and it is at this stage that the detail and degree intrusiveness of how each of these topic matters is authorised in relation to the identified person, with that authorisation open to be made by the Director-General.

---

[9] See definition of surveillance device as (a) a listening device, an optical surveillance device or a tracking device (b) a device that is a combination of any 2 or more of the devices referred to in paragraph (a) or (c) or (c) a device of the kind prescribed by regulation for the purposes of this paragraph

[10] See proposed s.26(2)(a,)(b) and (c) of the Bill.

[11] Explanatory Memorandum to Bill, 82.

[12] Explanatory Memorandum to Bill, 82; PJCIS Report, 115 Recommendation 29.

[13] See proposed s.27C (2) of the Bill, namely that the Minister is satisfied that "(a) the person is engaged in or is reasonably suspected by the Director-General of being engaged in, or of being likely to engage in, activities prejudicial to security and (b) the issuing of the warrant in relation to the person will, or is likely to, substantially assist the collection of intelligence relevant to security"

[14] See proposed s.27C (3)(c) of the Bill.

These amendments have two major implications. First, the scheme provides simply for a *broad shell or framework conditional approval by the Attorney General against an identified person*, with the specificity of detail of warrant operations and their application to be worked out later. In the practical context of approving the warrant (given that the specificity of detail will follow at a later time), this structure will actively encourage the giving of conditional approval for the Organisation *to do all* of the activities identified in s.27C (3)(c) (i) to (v) of the Bill, deferring final activation of these processes (and thus leaving a range of options open) to the second stage test, with authorisation open to the Director General. As such, the Bill confers a greater level of ultimate discretion.

Most remarkable is that activities and methods previously incorporated in the warrant approval itself by the politically accountable figure, the Attorney General, are now potentially devolved to the Director General,[15] not directly accountable to the Parliament. In turn, this subsequent authorisation of the range of activities that may be done under the identified person warrant is by reference to a broadly based test, with the Director General potentially the decision maker, as having to be "satisfied, on reasonable grounds, that doing that thing or those things under the warrant in relation to [subject content of the identified person warrant] will substantially assist the collection of intelligence relevant to the *prejudicial activities* of the identified person".

The phrase "prejudicial activities" provides no substantial limitation upon, or narrowing of, the scope of the warrant – as it is defined in s.22 of the Bill as meaning "activities prejudicial to security that the person is engaged in, or is reasonably suspected by the Director-General of being engaged in, or of being likely to engage in."

That this two-stage structure for warrants involving substantial devolution to the Director General appears to be driven *by operational considerations and efficiency objectives* (and in so doing, undermining the direct political accountability of the Attorney General) is confirmed by the fact that this immediate definition of "prejudicial activities" for authorising *operation of the warrant* is exactly the same language of the test engaged by the Minister for the *issue* (with conditional approval) of an identified person warrant, namely that "The Minister is only to issue an identified person warrant in relation to the person if he or she is satisfied that (a) the person is engaged in or is reasonably suspected by the Director-General of being engaged in, or of being likely to engage in, activities prejudicial to security".

Far from being a stricter accountability test, the second stage test merely reflects the devolution and deferral of the specificity and detail of warrant operations to the Director General and increases operational flexibility and discretion.

Again, convenience, flexibility and increased executive discretion (and reducing the documentary workload in the level of involvement by the Attorney General in the warrant approval process) are insufficiently proportional reasons to support the reforms as currently proposed given the intrusiveness and multiplicity of the surveillance measures contemplated.

---

[15] The relevant language used for authorisations under these warrants is that " Subject to subsection (3), the Minister or *Director General* may, on request, authorise the Organisation to do one or more of the following things under the identified person warrant in relation to…(see proposed ss 27D, 27E, 27F, 27G and 27H of the Bill)

. Accessing third party computers

Recommendation 22 of the PJCIS report recommends amendment of the *ASIO Act 1979* (Cth) to allow ASIO access to third party computers and communications in transit to access a target computer under a computer access warrant, "subject to appropriate safeguards and accountability mechanisms"[16]

Given that the target computer may be owned or used by persons with no involvement in matters of a security interest, the access to such third party computers and communications in transit as a means of accessing relevant data deserves the strictest regulation, and should be only permissible in exceptional or last resort circumstances where no other practicable alternative exists for accessing the security related data in the target computer.

The proposed amendment as paragraph 25A(4)(a) of the Bill *fails to set the threshold for use of another computer or a communication in transit to access the relevant data at a sufficiently high level* – simply, regard is to be had to other methods (if any) of obtaining access to the relevant data which are likely to be effective, and then merely that it is reasonable in all the circumstances to do so, to use the third party computer or third party communication as the point of access. This legislative drafting fails to ensure that it is absolutely necessary to access the security related data via third party means. .

This threshold should be raised to require direct consideration of other methods of obtaining access to the relevant data *not involving this third party intrusion*, and that such other methods need be positively ruled out as ineffective, or likely to be ineffective, in obtaining such relevant data. Only then in such exceptional and last resort circumstances should there be any capacity under warrant to use the third party computer or third party communication to enable access to the security related data.in the target computer.

. Variation of warrants and renewal of warrants

Recommendation 23 of the PJCIS report recommends the Government amend the warrant provisions of the *ASIO Act 1979* to promote consistency by allowing the Attorney General to vary all types of ASIO Act warrants.[17] Recommendation 25 of the PJCIS report recommends that the *ASIO Act 1979* be amended to allow the Attorney-General to renew warrants.[18]

The inclusion of proposed s.29A in the Bill unfortunately combines both variation to warrants and extensions to warrants, by treating a warrant extension as a variation – in s.29A (3) of the Bill, reflecting a level of conceptual confusion. Instead, it was contemplated that variations to warrants would involve "a relatively minor change in circumstances,"[19] in contrast to the quite significant change in circumstances of extending for up to six months the application of a panoply of intrusive surveillance powers under warrant.

There is no justification in mere Organisational administrative convenience and efficiencies to relax the present standards demanded by a fresh warrant application process at the expiration of each warrant, particularly as the reach and methods of the warrant are already contemplated in the Bill to be expanded by the introduction of the named person warrant and increases in access to third party computers and third party information transmissions under the computer access warrants.

---

[16] PJCIS Report , 95.
[17] PJCIS Report, 98
[18] PJCIS Report, 104
[19] A-G's Department Submission, cited in PJCIS Report, 97.

The present fresh application process underpins an internal accountability process focused upon periodically re-stating and justifying a plausible case for the use of intrusive surveillance powers and accordingly, periodically informing the Attorney General of a substantiated and continuing case why the collection of such intelligence, and the range of methods adopted for the collection of such intelligence, is relevant to the legal definition of security in the *ASIO Act 1979* (Cth). Such periodically renewed and updated awareness of the relevant intelligence case is an important step in the ministerial accountability arrangements underpinning the central role of the Attorney General in the *ASIO Act 1979* (Cth), which was in 1979 a deliberate choice over a judicially authorised warrant system.

It is also *an important economic efficiency measure* in ensuring that the resources and priorities of the Organisation are properly deployed and periodically re-assessed to match substantiated and prioritised ongoing security needs.

The present limited and discretionary content of the request by the Director-General in proposed s.29A (4) of the Bill, namely that the "request by the Director-General must specify (b) *where appropriate* - the grounds on which the Director-General suspects a person of being engaged in or reasonably suspected by the Director-General of being engaged in, or of being likely to engage in, activities prejudicial to security" fails to even formally require, for example, renewed assessment and review of the other limbs of the initial warrant tests.[20]

Accordingly, the proposed section of the bill should be re-drafted to make clear that warrants need to be renewed through a fresh application process and this process should be in a discrete section of the *ASIO Act 1979* (Cth).

In addition, an indicative list of authorised typical and genuine *minor variations* for the approval of the Attorney General should be written into the Bill, the defining line being that these are of a genuine administrative and not substantial nature. Again, the process for minor variations (which should not exceed the expiration of the existing warrant) should be in a discrete section of the *ASIO Act 1979* (Cth)

Schedule 5: Activities and Functions of *Intelligence Services Act* 2001 agencies

[20] For example, s.26(3)(a)(ii), (b)(i)and(c)(i) in relation to surveillance device wararnts; and for example, s.27C (2) in relation to identified Person Warrants

In responding to the inquiry's purpose as to whether the Bill appropriately implements the recommendations agreed by the Committee …and to assess the balance of national security and safeguards proposed in the Bill,"[21] it can be observed in general terms that Schedule 5 of the Bill also significantly expands the role and powers of ASIS, whilst continuing the pattern of devolution of decision making authority from the Attorney General (as responsible minister in relation to ASIO in interactions with ASIS) to the Director General, and with *further delegations* of power in the scheme from the Director General to other members of ASIO, described as "a senior position holder, or class of senior position holders"[22]

Schedule 5 accordingly proposes a liberalisation of intelligence production and communication of that intelligence on Australian persons, whilst simultaneously removing the responsible Ministers – for ASIS and ASIO - from some key decision making roles in operating the scheme under s.13B of the Bill. It provides a discretion – not an obligation – for the Ministers responsible for ASIO and ASIS to jointly make written guidelines concerning the activities under s.13 B of the Bill.[23]

. Expanding the power of ASIS under the Ministerial authorisation scheme of s.8 and s.9 of the *Intelligence Services Act 2001* (Cth) to produce intelligence on an Australian person

The Bill institutes a Ministerial authorisation scheme for ASIS for purposes for producing intelligence on an Australian person in relation to "activities that pose a risk, or are likely to pose a risk, to the operational security of ASIS."[24] The "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. [25]

Two issues clearly emerge. First, responding to interference by a foreign person or entity in operations undertaken by ASIS (which now includes certain ASIS operations within Australia, such as assistance to, and co-operation with ASIO) is already properly the concern of ASIO within the meaning of "security" within s.17 and s.3 of the *ASIO Act 1979* (Cth), in particular the s.3 definition (a) (i) espionage (ii) sabotage and (vi) acts of foreign interference, whether directed from, or committed within, Australia or not. The proposal arguably therefore duplicates existing powers and capacities to respond to such operational security issues- the protection of the integrity of ASIS operations is accordingly best addressed under these existing warrant based powers.

Second, inclusion of (b) reliance on inaccurate or false information is an extraordinarily vague, ill-defined and wide-ranging concept. What sort of inaccurate or false information from an Australian person might then satisfy the threshold requirement to be labelled a risk or likelihood of a risk to the operational security of ASIS, so as to meet the threshold for a Ministerial authorisation to produce intelligence on an Australian person?

Accordingly (b) should be deleted, or in the alternative, qualified *so as to exclude from the definition* of "inaccurate or false information" matters falling within the Commonwealth Constitution doctrine

[21] Media Alert PJCIS 18 July 2014
[22] Proposed s.13 C (1) of *Intelligence Services Act 2001* (Cth)
[23] See proposed s.13G of the Bill.
[24] Through the insertion of s.9(!A) (a) (iii) in the Bill into the *Intelligence Services Act 2001* (Cth)
[25] Definition to be inserted by the Bill into s.3 of the *Intelligence Services Act 2001* (Cth)

of the implied freedom of political communication and other matters of Australian persons engaging in lawful advocacy, protest or dissent, in relation to such information matters as they pertain to ASIS.

In addition, if not deleted, (b) should be further amended to more accurately reflect the more restricted Recommendation 38 of the PJCIS Report, namely 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".[26]

. Expanding ASIS activities undertaken in relation to the support ASIO without the requirement of Ministerial approval, under s.13B

It is difficult to see the need for these additional powers which enlarge the capacity of ASIO and ASIS to *act without ministerial authorisation* to undertake an activity or series of activities "for the specific purpose, or for purposes which include the specific purpose, of producing intelligence on an Australian person *or a class of Australian persons*"[27] .

The only plausible explanation appears to be executive and agency convenience, flexibility and discretion, and a weakening of the model of Ministerial responsibility for some activities of ASIS and ASIO in the production of intelligence on an Australian person.

Powers already exist under the Ministerial authorisation scheme in s.9 of the *Intelligence Services Act 2001* (Cth) to produce intelligence on an Australian person if the relevant Minister is satisfied that the Australian person is, or is likely to be involved in (iii) activities that are, or are likely to be, a threat to security[28] and the co-operative nature of these Ministerial arrangements is confirmed by the agreement of the Attorney General , as the responsible Minister for ASIO, in the authorised arrangements.[29]

The scheme proposed in Schedule 5 of the Bill makes clear that the proposed s.13 B takes effect *outside of the existing scheme in s.9 of the Intelligence Services Act 2001 (Cth), [30] and its system of ministerial authorisation, control and accountability.*

There are several objectionable and far reaching implications – commencing with the excessive scope of proposed s.13 B of the Bill, which appears to far exceed the context in which the *PJCIS Report* discusses the issue, (which was premised upon the existence and continuation of Ministerial authorisation arrangements)[31] and obfuscates the central issue of accountability by raising the matter of differences in legislative regimes between the two agencies.

---

[26] PJCIS Report, 134.
[27] Proposed S.13B (1) (a) amendment to *Intelligence Services Act 2001* (Cth) in the Bill.
[28] S.9(1A) (a) (iii) of the *Intelligence Services Act 2001* (Cth)
[29] Ss.9 (1A) (b) of the *Intelligence Services Act 2001* (Cth) states that the minister responsible for ASIS must "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 (whether or not covered by another subparagraph of paragraph (a) in addition to subparagraph (a) (iii) – obtain the agreement of the Minister responsible for administering the *Australian Security Intelligence Organisation Act 1979*".
[30] The amending s.13 B (5) states that "ASIS may undertake an activity or series of activities under subsection (1) without an authorisation under section 9 for the activity or series of activities.
[31] See PJCIS Report, 135 and Recommendation 39.

Second, the proposed S.13B abandons Ministerial approval where ASIS is undertaking an activity for the production of intelligence on an Australian person or class of Australian persons "to support ASIO in the performance of its functions"[32] and the activity or series of activities will be undertaken outside Australia.[33] Therefore proposed S.13 B diminishes the significance of this process to an executive based operational matter as the process of intelligence collection is instigated by the Director General or a senior ASIO position holder authorised by the Director General notifying ASIS that "ASIO requires the production of intelligence on the Australian person or class of persons". In turn, a senior ASIO position holder is broadly and liberally defined.[34]

Further still, ASIS need not receive such a request from ASIO where a staff member of ASIS, authorised by the Director General[35]and who will be undertaking the activity "reasonably believes that it is not practicable in the circumstances for ASIO to notify ASIS [in accordance with paragraph (d)] before undertaking the activity.[36]

These multiple levels of devolution and delegation make for both a weak accountability structure, and arguably creating an independently franchised and freelance capacity of ASIS to invoke powers to produce intelligence on an Australian person or class of Australian persons, independently assessing what falls within the rubric of ASIO functions, which is its function to support.

Effectively, the carefully crafted system of co-operative, Minister authorised arrangements between ASIS and ASIO under the existing s.9 scheme in the *Intelligence Services Act 2001* (Cth) can be sidestepped or circumvented. In addition, whole groups of Australian persons – "class of Australian persons" [37]are now brought within the intelligence production targeting, without any real specificity as to the particular identifying characteristics of such a "class of Australian persons".

Similarly, the proposed S.13 B amendment is so loosely drafted that the ASIO "functions" to which ASIS support is applied are apparently not restricted to the "functions" of ASIO as set out in s.17 of the ASIO Act 1979 (Cth) of functions in relation to "security" – 'security" itself defined in section 4 of the *ASIO Act 1979* (Cth).

This is because proposed s.13 B (5) states that "ASIS may undertake an activity or series of activities …without authorisation under section 9 for the activity or series of activities". Section 9 (1A) (a) of the *Intelligence Services Act 2001* (Cth) lists subject matter paragraphs (i) to (vii), of which *only paragraph (iii) relates to "security"* as defined in the *ASIO Act 1979* (Cth).

Furthermore, the potential circumvention of checks and balances and accountability measures in relation to ASIO's *domestic intelligence gathering function in relation to the legislated concept of security* – provided for in *the warrant authorisation process* for special powers in Part III, Division 2 of the *ASIO Act 1979* (Cth) (itself the subject of proposed modification by the *National Security Legislation Amendment Bill (No 1) 2014* and as examined above) – is evidenced by the proposed amendment to s.13B (6) of the *Intelligence Services Act 2001* (Cth).

---

[32] S.13B (1)(c) proposed amendment to *Intelligence Services Act 2001* (Cth).
[33] S.138 (1)(b) proposed amendment to *Intelligence Services Act 2001* (Cth)
[34] See S.4 proposed amendment to *ASIO Act 1979* (Cth): "means an ASIO employee, or an ASIO affiliate, who holds, or is acting in, a position in the Organisation that is (a) equivalent to or higher than a position occupied by an SES employee; or (b) known as Coordinator
[35] S.13B (3) and s.138 (7) – the Director General is also able to authorise a class of staff members of ASIS for these purposes
[36] S.13B (3) proposed amendment to *Intelligence Services Act 2001* (Cth)
[37] S.13B (1)(a) proposed amendment to *Intelligence Services Act 2001* (Cth)

Headed "*Incidental production of intelligence"* it states that "An activity or series of activities does not cease to be undertaken (b) for the specific purpose of supporting ASIO in the performance of its functions …only because, in undertaking the activity or series of activities, ASIS also *incidentally produces* intelligence that relates to the involvement, or likely involvement, of an Australian person in one or more of the activities set out in paragraph 9(1A)(a)".

This incidental production of intelligence may comprise matters of a purely domestic security matter, which ordinarily would be properly sought through the methods and techniques of the warrant based accountability mechanisms of Part III, Division 2 of the *ASIO Act 1979* (Cth) involving Ministerial approval.

In particular, the proposed s.13B is structured in such a way as to possibly encourage ASIS activities in support of ASIO for the prospective intelligence (however assessed of incidentally collecting intelligence through a process not subject to the requirements of warrant based approvals where, following conventional methods, warrant based approvals (with a higher standard of accountability) acquired.

The reform as presently structured potentially encourages the speculative undertaking by ASIS of activities in relation to ASIO as a means of producing incidental intelligence without being subject to the Part III, Division 2 *ASIO Act 1979* (Cth) warrant system.

Schedule 6: Protection of Information: higher penalties for existing offences and a range of new offences applying to intelligence agency information.

In responding to the inquiry's purpose as to "whether the Bill appropriately implements the recommendations agreed by the Committee …and to assess the balance of national security and safeguards proposed in the Bill,"[38] it can be observed that the proposed provisions in Schedule 6 relating to the protection of national security information are informed by two contemporary emphases, as revealed in the Explanatory Memorandum to the *National Security Legislation Amendment Bill (No 1) 2014*.

The first is in the multiplicity of offences and penalty increases, with four key amendments to the ASIO Act and the Intelligence Services Act[39] - comprising a total of 18 amendments involving either increased penalties or new offences.

The second is the assertive, exemplary directed and urgent language in the Explanatory Memorandum which frames the Schedule 6 reforms (but without specific naming of incidents) within the context of

[38] Media Alert PJCIS 18 July 2014

[39] See Explanatory Memorandum to Bill, 129, being (a) an increase in maximum penalties from two years to ten years imprisonment applying to offences of unauthorised communication in the both Acts; (b) extending the unauthorised communication offences in the Intelligence Services Act to the Office of National Assessments and the Defence Intelligence Organisation; (c) the inclusion of new offences applying to all Australian Intelligence Community agencies regarding intentional unauthorised dealings – such as intentional unauthorised removal, retention, copying or transcription- where the dealings stop short of an unauthorised communication of information to a third party; and (d) the inclusion of new offences in respect of intentional unauthorised recording of certain information or matter.

international disclosures of national security related information through Wikileaks, Edward Snowden and Chelsea (Bradley) Manning and the consequences arising thereof for Australian intelligence agencies:

> These amendments will ensure that the secrecy offences in the ASIO Act and the IS Act target, denounce and punish appropriately the wrongdoing inherent in the intentional unauthorised communication of, or dealing with, official records of information of AIC agencies…Recent domestic and international incidents involving the unauthorised communication of security intelligence-related information illustrate that the existing maximum penalty …does not accurately reflect the risk of serious harm to intelligence and security interests that is occasioned by such behaviour. Such risks include jeopardising extant intelligence-gathering operations …or investigations or prosecutions reliant upon intelligence information. The intentional unauthorised communication of intelligence information also risks compromising Australia's intelligence gathering capabilities by undermining relationships of trust and confidence with foreign intelligence partners and human sources.[40]

This statement and similar subsequent statements[41] present the ambit claim of Government interest in the protection and retention of intelligence agency information. Nonetheless, the sentiments in it, translated into the legislative drafting of the offences, do not appropriately reflect existing accountability requirements for intelligence agencies, given both the expansion of their mandates under the *National Security Legislation Amendment Bill (No 1) 2014*, the multiplicity of offences created and indeed, fairly recently introduced accountability mechanisms in the *Public Interest Disclosure Act 2013* (Cth).

The Explanatory Memorandum to the Bill makes brief reference of the Bill's interaction with two other legislated accountability mechanisms,[42] including the public interest disclosure regime in the *Public Interest Disclosure Act 2013* (Cth).

Under s.34 of this Act, an authorised internal disclosure where the disclosure relates to an intelligence agency[43] may be made to an authorised officer, for the purposes of s.34 of the Act, is an authorised internal recipient of the disclosure – in this instance, where the discloser believes on reasonable grounds that it would be appropriate for the disclosure to be investigated by IGIS- the Inspector General of Intelligence and Security becomes the authorised internal recipient.

The existing offences to be amended by the Bill[44] and the new offences to be introduced by the Bill[45] are each structured in a manner (with phrases adapted to the individual circumstances) as follows to exclude certain circumstances from the elements and constitution of the instant proposed or existing offence:

. "**the relevant conduct was not engaged in by the person**": *ASIO Act* s.18A (1)(e); *Intelligence Services Act* S.40C(1)(d), S.40E(1)(d),S.40G(1)(d), S.40H(1)(d) and S.40L(1)(d)

---

[40] Explanatory Memorandum to Bill, 130-131.
[41] See Explanatory Memorandum to Bill, 131-132.
[42] See Explanatory Memorandum to Bill, 132 paragraphs 687 and 688.
[43] S.8 of the *Public Interest Disclosure Act 2013* (Cth) defines intelligence agency as meaning ASIS, ASIO, DIGO, DIO, DSD and ONA.
[44] S.18 of the *ASIO Act 1979* (Cth) and sections 39, 39A and 40 of the *Intelligence Services Act 2001* (Cth)
[45] S.18A and 18B of the *ASIO Act 1979* (Cth) and s.40 A to s.40 M of the *Intelligence Services Act 2001* (Cth)

. "**the record is not made by the person**": *ASIO Act* s.18B(1)(e); *Intelligence Services Act* s.40D(1)(d), s.40F(1)(d), s.40H(1)(d), s.40K(1)(d) and s.40M(1)(d)

. "**the communication was not made**": *Intelligence Services Act* s.39(1)©, s.39A(1)(c), S.40(1)(c), s.40A(1)(c), and s.40B(1)(c)

The Bill should accordingly be modified to include under each of these clauses dealing with the communication of information, dealing with records, and the recording of information or matter – as applying individually to the six intelligence agencies - **that such activities were done as part of , or in preparation for, disclosure to the Inspector General of Intelligence and Security under sections 26, 33 and 34 of the *Public Interest Disclosure Act 2013* (Cth) (as a public interest disclosure to an authorised internal recipient).**

This amendment would then make clear that persons within the intelligence services so acting are immunised from criminal, civil and administrative liability under s.10 of the *Public Interest Disclosure Act 2013* (Cth), with necessary amendments.

I would be pleased to provide the Parliamentary Joint Committee with further information in relation to this submission, or to attend a public hearing of the Parliamentary Joint Committee in relation to this submission.

Yours faithfully

Dr Greg Carne
Associate Professor in Law
School of Law
University of New England
Armidale NSW 2351