

Submission to the Parliamentary Joint Committee of Intelligence and Security
Review of the National Security Legislation Amendment (Comprehensive Review and Other Measures No. 2) Bill 2023

Outline and Summary

Thank you for the opportunity to make a submission to the public consultation on the proposed Review of the National Security Legislation Amendment (Comprehensive Review and Other Measures No. 2) Bill 2023 (Cth) (“the Bill”).

This submission has been prepared in my capacity as a Senior Research Fellow of the T.C. Beirne School of Law at the University of Queensland. However, the views expressed below are entirely my own and are not representative of the School of Law, The University of Queensland or any other government, organisation or agency.

This submission addresses several challenges if the Bill was to be enacted in its present form. I have considered only certain sections and not provided comment on all sections in the Bill. However, the absence of specific statements in this submission should not be taken to be either an endorsement or rejection of those sections.

The aim of the Bill is to enhance the legislative framework of the National Intelligence Community (“NIC”) by implementing recommendations 18, 19, 66, 136, 145, 167, 186, 188, 191 and 192 of the *Comprehensive Review of the Legal Framework of the National Intelligence Community* (“the Richardson Review”).

I am happy to provide further clarification on any area of the submission.

Changes to the scope of substituted reference orders

Part 1 of the Bill introduces amendments to the *Law Officers Act 1964* (Cth) to repeal subsection 17(6) and replace it with a section that prohibits the delegation of the Attorney-General’s powers under both the ASIO Act¹ and the TIA Act. This amendment is strongly supported to ensure that only the Attorney-General, as the Commonwealth’s First Law Officer, can authorise the exercise of significant powers available to ASIO under the ASIO and TIA Acts. That amendment also accords with the findings of the Richardson Review.²

The Bill also proposes inserting a new section into both the *Australian Security Intelligence Organisation Act 1979* (Cth) (“the ASIO Act”)³ and the *Telecommunications (Interception and Access) Act 1979* (Cth) (“the TIA Act”),⁴ as well as inserting a note into the *Acts Interpretation Act 1901* (Cth), s 19B(2).

¹ Except for sections 34JE(3) and (4), which relate to determination of applications for financial assistance in respect of the subject of a questioning warrant's appearance before a prescribed authority for questioning under the warrant. This is an appropriate carve out for delegation.

² Richardson Review, vol 1, p 315, [14.46].

³ Section 5B.

⁴ Section 6V.

Collectively these provisions would limit the circumstances in which the Governor-General can make a substituted reference order under the ASIO Act or the TIA Act. The text of the proposed limitation is:

Unless the Prime Minister is satisfied that exceptional circumstances exist, the Governor-General must not make a substituted reference order under subsection 19B(2) of the *Acts Interpretation Act 1901* that relates to a provision of this Act (other than section 34JE) that refers to the Attorney-General.

It is worth observing that substituted reference orders are administrative instruments that cannot themselves alter the operation of statute. Instead, they are used to support Prime Ministerial decisions to abolish or create a particular authority, or to change or reallocate functions between authorities, in a way that supports the ongoing provision of government services.

Substituted reference orders may also be disallowed under the ordinary process provided for by the *Legislation Act 2003* (Cth)⁵ and Parliamentary Standing Orders.

Despite those observations, there are two dangers with the proposed amendment.

Firstly, the provision would permit the Prime Minister to seek a substituted reference order which would circumvent the Attorney-General's approval for the exercise of powers under the ASIO and TIA Acts for nothing more than unspecified 'exceptional circumstances'. In recent years, the Prime Minister has cited the 'exceptional circumstances' of the COVID-19 pandemic to seek the Governor-General's approval of appointments across multiple Ministerial portfolios.⁶ Without clarity on what would constitute an 'exceptional circumstance', this text could impermissibly permit circumvention of the Attorney-General in the exercise of powers under the ASIO or TIA Acts without proper cause. The Richardson Review itself indicated that exceptional circumstances could only be satisfied by something as serious as 'where there is no Attorney-General'.⁷

Secondly, the provision hinges the making of a substituted reference order on the satisfaction of the Prime Minister (as applicant) that exceptional circumstances exist, rather than the Governor-General (as decision-maker). Whilst section 19B(2) is a discretionary power afforded the Governor-General, and therefore permits the Governor-General power to refuse to make a substituted reference order in any given circumstances, it would be more appropriate for the provision to reflect that the Governor-General must be satisfied that exceptional circumstances exist before making a substituted reference order in relation to the Attorney-General under the ASIO and/or TIA Acts.

Amendment of immunities for telecommunications offences

Part 2 of the Bill then a series of defences for certain 'national infrastructure-related offences'. Section 5 of the Bill introduces the definition of 'ASIO officer' into the *Criminal Code* (Cth) ("the Code"),⁸ which would have the effect of applying the definition across all of the offences in Part 10.6. Section 6 of the Bill then absolves ASIO officers of the offence of 'interference with facilities' under section 474.6 of the Code if they act in good faith and the conduct is 'reasonable in the circumstances for the purpose of performing that duty'.

⁵ s 42.

⁶ Stephen Dongahue QC, *In the Matter of the Validity of the Appointment of Mr Morrison to Administer the Department of Industry, Science, Energy and Resources* (Opinion SG12 of 2022) <<https://www.pmc.gov.au/sites/default/files/media-releases/sg-no-12-of-2022.pdf>>.

⁷ Richardson Review, vol 1, 315, [Recommendation 19].

⁸ At s 473.1.

An immunity is also enacted in respect of the computer offences in Part 10.7 of the Code for the offences of ‘unauthorised modification of data to cause impairment’ and ‘unauthorised impairment of electronic communication’.⁹

Ordinarily, interferences with infrastructure of the kind contemplated by the offence provisions of the Code would be authorised by a warrant under the ASIO Act.¹⁰ However, the evidence before the Richardson Review was that such activities were occasionally performed without a warrant ‘some of the activities for which ASIO needs protection from criminal liability are done in the very early stages of an investigation’.¹¹

The first danger is the wide-ranging nature of immunities as they apply to persons who are not ASIO employees. An ASIO affiliate is defined in the ASIO Act as ‘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’.¹² Because sections 85 and 87 do not limit down who may be considered an ASIO affiliate, there is the potential for ASIO immunities to apply to the domestic actions of other officers of agencies of the Executive such as the AFP, ASIS or other NIC law enforcement agencies in circumstances that would ordinarily require a judicially approved warrant. The Richardson Review only recommended the extension of these immunities to ASIO officers.¹³

It is also worth noting that the immunities which the Code provides to ‘law enforcement officers’¹⁴ does not ordinarily include affiliates of law enforcement agencies. Further, the term ‘intelligence or security officer’ already exists in the Code in relation to qualified defences, and includes all employees of ASIO, ASIS, ASD, ONI and DIO as well as contractors of those agencies.¹⁵ The policy need to incorporate ASIO affiliates as a further category of immunised person is not addressed in the Explanatory Memorandum nor the Richardson Review.

The second danger is that it is unclear whether the proposed immunity would cover the Australian Defence Force (“ADF”). The Richardson Review was of the view that ‘a limited immunity is necessary and justified in respect of the ADF... where the ADF is properly authorised to engage in activity that could raise potential liability risks under Australian criminal law... but cannot access ASD authorities and immunities’.¹⁶ The proposed immunity *per se* does not immunise ADF members; however, there is nothing in the law that would prevent an ADF member from being engaged as a consultant¹⁷ or as a service provider.¹⁸ Further, the immunity would not automatically attach to an ADF member taking part in a special intelligence operation authorised under the ASIO Act.¹⁹ The coverage of ADF

⁹ The Bill, ss 7, 8 and 9.

¹⁰ For example ASIO Act, ss 25A, 26B, 27A and 27E.

¹¹ Richardson Review, vol 2, 189-190

¹² At s 4.

¹³ Richardson Review, vol 1, 68 and vol 2, 188-191.

¹⁴ The Code, s 473.1 and the *Crimes Act 1914* (Cth), s 3(1). See also the Code, s 146.1 for the definition of “Commonwealth law enforcement officer”.

¹⁵ The Code, s 473.1 and *Intelligence Services Act 2001* (Cth), s 3(1).

¹⁶ Richardson Review, vol 1, 51.

¹⁷ ASIO Act, s 85.

¹⁸ *Ibid*, s 87.

¹⁹ *Ibid*, s 4.

personnel under the proposed immunities should be clarified (i.e., whether they are intended to be immunised or that will be dealt with by subsequent legislative amendment).

Changes to spent convictions law

In Part 4 the Bill also seeks to amend the *Crimes Act 1914* (Cth)²⁰ to the extent that spent convictions information²¹ can be handled by and on behalf of ASIO.

ASIO (indeed all of the NIC agencies) already receive the benefit of an exemption to spent convictions law under s 85ZZH in respect of ‘prospective employees’ and ‘persons proposed to be engaged as consultants to, or to perform services’. The proposed amendment would allow ASIO the same degree of access to spent convictions as law enforcement agencies currently enjoy under s 85ZZJ.

This recommendation is supported in principle; however, the difficulty is the drafting of the purposes of use of spent convictions information. To clarify, the existing s 85ZZJ – which authorises disclosure of spent conviction information to law enforcement agencies – does permit use of spent conviction information. However, it limits the ‘use’ to which spent convictions information may be used to ‘the investigation or prevention of crime, where the investigation or prevention of crime is a function of the agency’.²² Therefore, the use of spent convictions information is only permitted where it involves satisfaction of two circumstances: 1.) the investigation or prevention of crime, and 2.) use by an agency that has a function of investigating or preventing crime.

The proposed amendments limit use of spent convictions information ‘for the purposes of the performance of the functions, or the exercise of the powers, of ASIO or the officer’. The difference between the terms may be minor – but creates foreseeable risks such as:

1. Obtaining spent convictions information of an Australian citizen for the purposes of generating ‘intelligence’, which is a permissible exercise of the functions of ASIO;²³
2. Sharing that intelligence (including the spent convictions information) with an agency not ordinarily authorised to receive it, such as ASIS, ASD, AGO or ONI²⁴ and circumventing these agencies’ need for a Ministerial authority for intelligence collection on Australian citizens.²⁵

The connection between the use of spent convictions information and the personal exercise of powers by ASIO officers (which would include ‘affiliates’ such as contractors and secondees) also raises the spectre of officers using spent convictions information in an unfettered manner. For example, an officer may use spent conviction information for the purpose of exercising a power under the ASIO Act without necessarily demonstrating a connection to furthering the purpose of any ASIO function under the ASIO Act.²⁶

For clarity, the provision should require that the use of spent convictions information under the proposed section 85ZZJA(1)(c) could only be for ‘the performance of the functions of ASIO, or the exercise of the powers of ASIO or the Director-General of Security’. This amendment would place appropriate fetters around the *purpose* for which spent convictions information could be used by

²⁰ *Crimes Act 1914* (Cth), s 85ZZJA.

²¹ *Ibid*, s 85ZV.

²² *Ibid*, s 85ZZJ(1)(c).

²³ ASIO Act, s 17(1)(a) and/or (e).

²⁴ *Ibid*, s 19A(1) and (2).

²⁵ *Intelligence Services Act 2001* (Cth), ss 8, 9, 13A and 13B.

²⁶ ASIO Act, s 17(1).

ASIO, and limit only the Director-General to the use of that information in the exercise of ASIO Act powers.

Exemptions from Freedom of Information

The amendments in Part 6 of the Bill would permit limited access under the Freedom of Information (FOI) scheme to certain hydrographic information possessed by the AGO and would also align the protections under the FOI scheme to suspicious matter reports and AUSTRAC intelligence documents (such as SMRs and SUSTRs) to those in the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth).

These amendments are reasonable and appropriate and are strongly supported.

Review of decisions in AAT

Part 8 of the Bill would amend the administrative appeals and archives legislation in a manner that would only require the Inspector-General of Intelligence and Security (IGIS) to appear and give evidence for reviews to access “exempt security records”. The amendments would also make clear that all national security determinations in the AAT would be heard in the Security Division.

These amendments are reasonable and appropriate and are strongly supported.

Amendment to Ministerial authorisations

Part 9 of the Bill makes an amendment to the *Intelligence Services Act 2001* (Cth) to permit the Minister to issue directions to ASIS which would expand on the functions of ASIS outlined in section 6(1) of that Act. The Minister may expand these functions only where they ‘an activity, or a series of activities, that will, or is likely to, have a direct effect on an Australian person’.²⁷ This is said to be needed to ‘provide certainty regarding the level of detail required to describe the directed activities in a Ministerial direction’²⁸ and noting that the proposed amendments remain subject to certain exemptions already in the Act.²⁹

It is worth noting that this amendment does not align with any specific recommendation of the Richardson Review. Recommendation 59 speaks to a need to ‘ministerial oversight and visibility of activities to achieve a direct effect undertaken directly by ASIS and ASD’, but did not recommend defining the term direct effect.³⁰ Indeed, this was noted as a key requirement of the proposed functions of ASIS in 2001:

...in cases where the responsible Minister may activate ‘other activities’ under 6(1)(e) which relate to Australian citizens or Australian organisations overseas, then further accountability is required. This can be achieved through connecting the operation of 6(1)(e) to clauses 8 and 9 of the IS Act which provide for Ministerial directions and authorisations.³¹

Firstly, the difficulty with the proposed amendment is that it seeks to disconnect the activities authorised by the Ministerial direction from their intended *purpose*. The Explanatory Memorandum

²⁷ *Intelligence Services Act 2001* (Cth), s 8(1)(a)(ii).

²⁸ Explanatory Memorandum to the National Security Legislation Amendment (Comprehensive Review and Other Measures No. 2) Bill 2023 (“Explanatory Memorandum”), 32.

²⁹ *Intelligence Services Act 2001* (Cth), ss 6(4), 6(5B), 8(1A), 11 and 12.

³⁰ Richardson Review, vol 2, 172, [Recommendation 59].

³¹ Joint Select Committee on the Intelligence Services, *An Advisory Report on the Intelligence Services Bill 2001, the Intelligence Services (Consequential Provisions) Bill 2001 and certain parts of the Cybercrime Bill 2001 (August 2001)*, paras 2.16-2.17; cited in Richardson Review, vol 2, 166.

mentions that this reference to purpose is the ‘practice to date’, which the amendment seeks to change.³² Yet the Richardson Review was keen to reinforce that this was precisely the point of the legislation:

The Review considers that the purpose for which an agency is undertaking an activity is paramount and should be brought to the minister’s attention at the time he or she is asked to authorise that activity.

It follows, therefore, that ministerial authorisation to produce intelligence is insufficient where an agency is, in fact, undertaking activities to achieve a direct effect in its own right. The Review does not think it is enough that the categories for seeking ministerial authorisation to produce intelligence contemplate or suggest that action will be taken by the relevant agency. In our view, the inference of a response to intelligence is simply not sufficient to ensure ministerial oversight and accountability for direct effects against an Australian person.³³

The purpose for which activities are being authorised must be enshrined in the legislation which gives effect to those activities. The purpose of exercising intrusive powers or undertaking direct effects against Australian citizens – no matter where they are in the world – is dependent on maintaining some semblance of distinction between the gathering of intelligence, the investigation of crime, and the exercise of foreign policy.³⁴

Consider, using the example from the Explanatory Memorandum (disruption of terrorism), that under the proposed amendments the actions of ASIS could:

- interfere in the movement of an individual outside Australia suspected of involvement in a terrorist attack;
- disrupt the supply of weapons to terrorist organisations outside Australia;
- degrade the capabilities of terrorist organisations outside Australia; or
- communicate information with a third party

irrespective of whether any or all of those actions, taken together or in isolation, actually achieve the underlying purpose of disrupting terrorism for which those activities were authorised. By proscribing that the Minister may specify a class of activities which ASIS may undertake, rather than a “class of purposes” for which activities could be pursued, the amendment impermissibly fragments the operation of the Ministerial direction.

Secondly, the proscribed amendment does not actually provide further detail about what the Minister is authorising. The Explanatory Memorandum states that ‘[w]here a class [of activities] has been specified by the Minister, ASIS will be responsible for satisfying itself that a proposed activity falls within the specified class’. This raises the possibility that – consistent with the example in the Explanatory Memorandum – the Minister merely provides a “ballpark” of possible options within which ASIS is constrained to operate. This does not achieve any greater level of clarity about exactly what activities ASIS can undertake.

Thirdly, there are further issues with the allocation of responsibility for assessing the lawfulness of activities to which the Minister may proscribe. The Explanatory Memorandum states that ‘[w]here a class has been specified by the Minister, ASIS will be responsible for satisfying itself that a proposed activity falls within the specified class’.³⁵ Given the highly volatile and uncertain environments in which

³² Explanatory Memorandum, 32.

³³ Richardson Review, vol 2, 171, [23.29] and [23.30].

³⁴ Brendan Walker-Munro, ‘The Richardson Review: Reviving the “Purpose” of Law Enforcement and Intelligence Legislation’ (2023) 46(1) *UNSW Law Journal* 268, 271.

³⁵ Explanatory Memorandum, 32.

ASIS operates offshore, it does not appear appropriate for the Minister to derogate responsibility for compliance in such a fashion, and may threaten either or both of the lives of ASIS officers or the operational integrity of their work. Instead, officers of ASIS should be free – subject to the existing restraints in the Act³⁶ – to pursue the activities that are operationally justified within the purpose set out in the Ministerial direction³⁷ and the Ministerial authorisation.³⁸

Conclusion

The Bill enacts a number of the recommendations of the Richardson Review, and is broadly supported for updating and clarifying a number of aspects of Australia’s NIC framework. However, there are also some challenges inherent in the proposed legislation which may need to be addressed before the Bill is passed.

Thank you for the opportunity to make this submission.

Dr Brendan Walker-Munro, Senior Research Fellow, The University of Queensland

[REDACTED]

³⁶ *Intelligence Services Act 2001* (Cth), ss 6(4), 6(5B), 8(1A), 11 and 12.

³⁷ *Ibid*, ss 6(1)(e) and 8(1)(a)(ii).

³⁸ *Ibid*, ss 9-9D.