Law Council
OF AUSTRALIA

Office of the President

7 February 2018

Mr Andrew Hastie
Chair
Parliamentary Joint Committee on Intelligence and Security
PO Box 6021
CANBERRA ACT 2600

By email: pjcis@aph.gov.au

Dear Mr Hastie,

Security of Critical Infrastructure Bill 2017

1. The Law Council welcomes the opportunity to provide this submission to the Parliamentary Joint Committee on Intelligence and Security (**the Committee**) regarding its review of the Security of Critical Infrastructure Bill 2017 (**the Bill**).

2. The Law Council acknowledges the assistance of its Foreign Investment Committee of Business Law Section (**the FI Committee**) and National Criminal Law Committee in the preparation of this submission.

3. The Bill, if enacted, would create two new measures designed to strengthen the Government's capacity to manage the national security risks of espionage, sabotage and coercion arising from foreign involvement in Australia's critical infrastructure, with minimal regulatory impact and maintaining Australia's open investment policy. The Bill will regulate approximately 140 assets across four high-risk sectors: electricity, water, gas and ports. The two measures are:

    a) Creation of a 'last resort' Ministerial directions power, which would allow the Minister to issue a direction to an owner or operator of a critical infrastructure asset to mitigate significant national security risks; and
    b) Creation of a critical assets register (**the Register**) that will provide the Australian Government with information relating to who owns, controls and has access to critical infrastructure assets most at risk from espionage, sabotage and coercion.

4. The Bill was drafted in consultation with the Treasury, the Federal Investment Review Board (**FIRB**) and the Critical Infrastructure Centre (**the Centre**). The Bill was further developed following consultations with state and territory governments and investors held by the Attorney-General's Department in March and June 2017, and public consultations following the release of an exposure draft bill in October 2017.

Telephone +61 2 6246 3788 • *Fax* +61 2 6248 0639 • *Email* mail@lawcouncil.asn.au
GPO Box 1989, Canberra ACT 2601, DX 5719 Canberra • 19 Torrens St Braddon ACT 2612
Law Council of Australia Limited ABN 85 005 260 622
www.lawcouncil.asn.au

5. The FI Committee previously provided a submission for the Critical Infrastructure Centre's Discussion Paper on Strengthening the National Security of Australia's Critical Infrastructure.[1]

6. This submission focused on the need for the Government to strike an appropriate balance between security concerns with legitimate investment activities without deterring bona fide foreign investment, and that foreign investors should be provided with greater clarity and upfront guidance as to which assets will be affected by the Bill, before investors commence spending significant amounts of time and costs preparing a bid.[2]

7. The Law Council is pleased the Bill provides: clear definitions of 'critical infrastructure asset',[3] to ensure the law is both readily known and available, and clear and certain, as consistent with the rule of law;[4] affords due process by allowing an entity to seek judicial review of the Minister's decision to issue a direction;[5] and safeguards on the Minister's exercise of the last resort directions power.[6]

Creation of a Register

8. The Bill creates a framework for keeping a register of information in relation to critical infrastructure assets. According to the Explanatory Memorandum, the Register would assist the Centre in fulfilling its key functions of identifying Australia's critical infrastructure, conducting national security risk assessments, developing risk management strategies in consultation with state and territory governments, regulators and critical infrastructure owners and operators, and supporting compliance.[7]

9. Under the Bill two sets of entities will be required to report – direct interest holders (greater than 10% direct in the asset or entities who otherwise hold a direct interest that puts the entity in a position to directly or indirectly influence or control the asset)[8] and responsible entities (body licensed to operate the asset).[9] An entity that is a direct interest holder may be an individual, a body corporate, a body politic, a partnership, a trust or superannuation fund, or an unincorporated foreign company.[10]

10. There are three areas of uncertainty around the scope of the definition of direct interest holder. The Law Council recommends that the three points below be addressed.

11. Firstly, it is not clear from the drafting whether a direct interest holder under proposed section 8 is limited to the immediate shareholder or interest holder of the asset or whether it could extend to intermediate or ultimate holding entities of the assets.

12. Secondly, it is not clear whether 'entity' in proposed subsection 8(1) is limited to the entities listed at proposed paragraphs 8(2)(a)-(d) or whether the entities listed in proposed

[1] Business Law Section, Law Council of Australia 'Strengthening the National Security of Australia's Critical Infrastructure Discussion Paper' (21 March 2017).
[2] The Law Council of Australia 'Strengthening the National Security of Australia's Critical Infrastructure Discussion Paper' (21 March 2017).
[3] Security of Critical Infrastructure Bill 2017 ss 9-12.
[4] The Law Council of Australia, *Policy Statement: Rule of Law Principles,* March 2011, Principle 1, 2.
[5] *Administrative Decisions (Judicial Review) Act 1977* s 5(1)(a).
[6] Security of Critical Infrastructure Bill 2017 ss 32(3), 33.
[7] Explanatory Memorandum Security of Critical Infrastructure Bill 2017 [7], [15]-[16].
[8] Ibid s 8.
[9] Ibid s 5.
[10] Security of Critical Infrastructure Bill 2017 s 5.

subsection 8(2) are in addition to the entities in the definition of 'entity' in proposed section 5 of the Bill. The Law Council recommends clarifying the drafting.

13. Thirdly, the definition of influence or control could cover ordinary course of business financing arrangements where financiers have a certain level of influence or control over the assets, whether or not the they have enforced their security. The Law Council recommends adding an express carve-out for moneylending agreements. See regulation 27 in the Foreign Acquisitions and Takeovers Regulation 2015 for an example.

14. Interest and control information is defined in section 6 of the Bill. It includes: the entity's name, Australian Business Number, address, country of residence or incorporation; the type and level of interest the entity has in the asset; information about the influence or control the entity is in a position to directly or indirectly exercise in relation to the asset, such as veto rights; and information about any person appointed by the entity who has direct access to networks or systems that are necessary for the operation or control of the asset.[11]

15. Operational information is defined in section 7 of the Bill. It includes information regarding the asset's location, description of the area the asset services, information regarding the entity that is the responsible entity for, or operator of, the asset, information about the chief executive officer, and a description of the arrangements in relation of the operation of the asset.[12]

16. A responsible entity for a critical infrastructure asset must give the Secretary operational information, and interest and control information, in relation to the entity and the asset.[13] If particular events occur in relation to the asset, the entity must also notify the Secretary.[14] Time limits apply for when the information must be given.[15]

17. The Register is not to be made public.[16] The information contained in the Register is protected information,[17] and civil penalties apply where an entity does not give information as required by the Bill.[18]

Privacy considerations relating to 'protected information' under the Register

18. The Bill states that interest and control, and operational information obtained under the Register may include personal information within the meaning of the *Privacy Act 1988*.[19] This means that the collection of any personal information must be consistent with the Australian Privacy Principles, (**APPs**) including ensuring the accuracy of personal information it collects,[20] and that this personal information is protected by reasonable security safeguards.[21]

---

[11] Ibid s 6(1)(a)-(i).
[12] Ibid s 7(1)(a)-(g).
[13] Ibid s 23.
[14] Ibid s 24.
[15] Ibid s 23(3) and s 24(2).
[16] Security of Critical Infrastructure Bill 2017 s 22.
[17] Ibid s 5.
[18] Ibid ss 23(2) and 24(2).
[19] Security of Critical Infrastructure Bill 2017 ss 6(2) and 7(2).
[20] *Privacy Amendment (Enhancing Privacy Protection) Act 2012,* schedule 1, part 4, section 10 – quality of personal information.
[21] *Privacy Amendment (Enhancing Privacy Protection) Act 2012,* schedule 1, part 4, section 11 – security of personal information.

19. The Office of the Australian Information Commissioner (**OAIC**) recommended in a submission to the Discussion Paper on Strengthening the National Security of Australia's Infrastructure that the Centre undertake a privacy impact assessment prior to the establishment of the Register to ensure that any risks to individuals' personal information are identified and mitigated.[22] In relation to entities disclosing to parties with which they will share personal information, the OAIC also recommend that in the interests of privacy best practice, when information is obtained the Centre and Secretary ensure that each entity is made aware of the need consider existing APP obligations.

20. The Law Council supports the recommendations of the OAIC, and that in administering the Register the Centre and Secretary continue to act in accordance with the APPs and in consultation with the OAIC.

Retention of documents

21. The Law Council notes that under section 39 of the Bill the Secretary may retain possession of documents obtained from reporting entities and operators of critical infrastructure assets as part of the Register, the Ministerial directions power, or as relevant to the assessment of a national security risk, for as long as he or she deems necessary.

22. The Law Council queries whether the Secretary's ability to retain documents for an unlimited time period may be inconsistent with APP 11.2. This requires that where an APP entity holds personal information, and they no longer need to the information for which it was used or disclosed by the entity, the entity must take reasonable steps to destroy the information or to ensure that the information is de-identified. [23]

23. To ensure that the Bill is consistent with APP 11.2, the Law Council recommends that section 39 of the Bill be amended to reflect the requirement that the Secretary must take reasonable steps to destroy the information when it is no longer necessary.

Threshold test for exercise of the 'last resort' Ministerial directions power

24. The Minister may give an entity that is the reporting entity for, or an operator of, a critical infrastructure asset a written direction requirement the entity to do, or refrain from doing, a specified act or thing within a specified period.[24] The Minister may only issue the direction if they are satisfied that there is a risk of an act or omission that would be prejudicial to security.[25]

25. The Bill includes a number of safeguards on the Ministerial directions power. The Minister must be satisfied that requiring the entity to do or refrain from doing a specified act is reasonably necessary to eliminate or reduce a risk,[26] reasonable steps have been taken to negotiate in good faith with the entity to reduce or eliminate the risk without a direction,[27] an adverse security assessment has been given,[28] and the Minister is satisfied that no

[22] The Office of the Australian Information Commissioner, 'Strengthening the National Security of Australia's Critical Infrastructure – A Discussion Paper – submission to the Critical Infrastructure Centre' (March 2017), available online at https://www.oaic.gov.au/engage-with-us/submissions/strengthening-the-national-security-of-australia-s-critical-infrastructure-a-discussion-paper-submission-to-the-critical-infrastructure-centre.
[23] *Privacy Amendment (Enhancing Privacy Protection) Act 2012,* schedule 1, part 4, section 11.2 – security of personal information.
[24] Security of Critical Infrastructure Bill 2017 s 32(2).
[25] Ibid.
[26] Ibid s 32(3)(a).
[27] Ibid s 32(3)(b).
[28] Ibid s 32(3)(c).

existing regulatory system of Commonwealth, a State or Territory could instead be used to eliminate or reduce the risk.[29] Before issuing a direction the Minister must also have regard to the adverse security assessment, the costs incurred by the entity in complying with the direction, the consequences for competition in the industry, the potential consequences the direction may have on customers of the services provided by the entity, and any representations given by the entity or consulted Minister.[30]

26. The Law Council supports the inclusion of safeguards in the Bill to ensure the Minister only exercises the directions power as a last resort, and only after negotiation in good faith with the affected entity, and consultation with the relevant State or Territory Minister. However, the Law Council has concerns that uncertainty remains regarding the threshold for the Minister to exercise the directions power, in particular the definition of 'prejudicial to security' and the Minister's consideration of an adverse security assessment.

27. The Law Council notes that existing investors in critical infrastructure often have negotiated existing contractual arrangements with the Commonwealth, State or Territory as to how the assets would be operated and regulated. It would be inappropriate to disregard these negotiated arrangements entirely in the exercise of the last resort power, as the investors could have committed their investments based on certain assumed arrangements. As such, the Law Council recommends that these existing arrangements be protected from adverse modification by a last resort direction or at least be taken into account as one of the factors in proposed subsection 32(4), in addition to the existing regulatory system of the Commonwealth, a State or a Territory referenced at proposed subsection 32(3) of the Bill.

Definition of 'prejudicial to security'

28. The Minister may only issue the direction if they are satisfied that there is a risk of an act or omission that would be prejudicial to security.[31] The Bill does not include a definition of 'prejudicial to security'. It adopts the broad definition of 'security' provided under section 4 of the Australian Security Intelligence Organisation Act 1979 (the ASIO Act) which means the protection of the Australian Government, states, territories and the people of Australia from espionage, sabotage, politically motivated violence, promotion of communal violence, attacks on Australia's defence system, or acts of foreign interference, as well as the protection of Australia's border integrity from serious threats. The Explanatory Memorandum states the term 'prejudicial to security':

> *… is to be given its ordinary meaning, but interpreted in a manner that is consistent with the term 'activities prejudicial to security' contained in the ASIO Act. As a matter of guidance only, activities prejudicial to security may cover activities relevant to 'security', as defined under the ASIO Act, that could be considered capable of causing damage or harm to Australia, the Australian people, or Australian interests, or to foreign countries to which Australia has responsibilities… to demonstrate the risk is prejudicial to security, consideration would be given to the specific threat posed, as well as the vulnerability and consequence of the risk.*[32]

[29] Ibid s 32(3)(d).
[30] Ibid s 32(4).
[31] Ibid s 32(1).
[32] Explanatory Memorandum, Security of Critical Infrastructure Bill 2017 [260]-[261].

29. The rule of law requires that the law must be both readily known and available and certain and clear.[33] This requires that key terms be defined.[34] To ensure that that the Minister's 'last resort' directions power under Part 3 Division 2 can only be exercised in the circumstances intended by the Explanatory Memorandum, the term 'prejudicial to security' should be defined in the legislation itself. This would also ensure that the term 'prejudicial to security' could not be later redefined without adequate Parliamentary scrutiny.

Adverse security assessments

30. Under proposed paragraph 32(2)(c) of the Bill, the Minister must not give a direction unless they have been given an adverse security assessment in respect of the entity.[35] Before giving the entity the direction the Minister must also have regard to the adverse security assessment.[36] The Minister must have regard to other matters,[37] however, the Minister must give the greatest weight to the adverse security assessment.[38]

31. An adverse security assessment is defined in section 35 of the ASIO Act. It means a security assessment in relation to a person that contains:

    a) any opinion or advice, or any qualification of any opinion or advice, or any information, that is or could be prejudicial to the interests of the person; and
    b) a recommendation that prescribed administration action be taken or not be taken in respect of the person, being a recommendation the implementation of which would be prejudicial to the interests of the person. [39]

32. The Law Council has previously expressed concern regarding adverse security assessments to the Attorney-General's Department in relation to the exposure draft Telecommunications and Other Legislation Amendment Bill 2015 (also known as the Telecommunications Sector Security Reform).[40] The issuing of an adverse security assessment is not required to be based on conventional standards of proof such as a 'balance of probabilities' test. The specific criteria by which the Australian Security Intelligence Organisation (**ASIO**) make their assessments are also largely unknown (beyond the fact for example that it must relate to ASIO's functions and the definition of security under section 4 of the ASIO Act), making it uncertain as to whether when a risk or threat to a critical infrastructure asset will be considered to be of a sufficient level of seriousness to warrant the issuing of a direction by the Minister.

33. For example, it is unclear whether a risk or prejudice to security must be substantial, likely, imminent or of severe potential impact before an adverse security assessment is issued.

---

[33] Law Council of Australia, *Policy Statement: Rule of Law Principles,* March 2011, Principle 1, 2.
[34] Ibid.
[35] Security of Critical Infrastructure Bill s 32(3)(c).
[36] Ibid s 32(4)(a).
[37] Matters etc. to which regard must be had are: the costs that would likely be incurred by the entity in complying with the direction (s 32(4)(b)); the potential consequences that that direction may have on competition in the relevant industry for the critical infrastructure asset (s 32(4)(c)); the potential consequences that the direction may have on customers of, or services provided by, the entity (s 32(4)(d)); any representations given by the entity or a consulted Minister under subsection 33(2) within the period specified for that purpose (s 32(2)).
[38] Security of Critical Infrastructure Bill s 32(5)(a).
[39] *Australian Security Intelligence Act 1979* (Cth) s 35.
[40] Law Council of Australia, 'Submission to the Attorney-General's Department on the exposure draft Telecommunications and Other Legislation Amendment Bill 2015' (18 January 2015), 2.

While merits review of ASIO's adverse security assessments would be available,[41] this will not necessarily indicate the criteria used in the issuance of a security assessment.

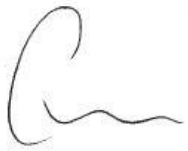
34. To ensure consistency with the rule of law, any process that may result in substantial impacts on entities and potentially the services provided to customers must be, to the extent possible, transparent.[42] The threshold for the exercise of the directions power should only be permitted where there is a sufficient level of risk to security to justify the exercise of the powers. This could be achieved, for example, by amending proposed section 32(3) of the Bill to require that the Minister is satisfied that there is substantial and imminent risk or unauthorised interference with, or unauthorised access to, a critical infrastructure asset that would be prejudicial to security.

Thank you for the opportunity to provide these comments.

The Law Council would be pleased to elaborate on the above issues, if required.

Please contact Dr Natasha Molt, Deputy Director of Policy, Policy Division (02 6246 3754 at Natasha.molt@lawcouncil.asn.au), in the first instance should you require further information or clarification.

Yours sincerely



Morry Bailes
President

[41] *Australian Security Intelligence Act 1979* (Cth) s 54.
[42] Law Council of Australia, *Policy Statement: Rule of Law Principles,* March 2011, Principle 1, 2.