Law Council
OF AUSTRALIA

Office of the President

16 September 2020

Mr Michael Pezzullo AO
Secretary
Department of Home Affairs
PO Box 25
BELCONNEN ACT 2616

Submitted via web form: www.homeaffairs.gov.au

Dear Mr Pezzullo

Submission: Protecting Critical Infrastructure and Systems of National Significance

1. The Law Council of Australia (**Law Council**) welcomes the opportunity to comment on the Department of Home Affairs' Consultation Paper, *Protecting Critical Infrastructure and Systems of National Significance* (**Consultation Paper**) released on 12 August 2020.[1]

2. The Law Council's response focuses on key attributes of the legislative amendments that would be necessary to implement the proposed regulatory regime.

3. In view of the limited timeframe for public submissions on the Consultation Paper and the limited information provided about the intended design of the proposed regulatory regime, the Law Council provides some general observations on matters of legislative design, to ensure consistency with fundamental rule of law principles.

4. Particular areas of focus include the exercise of coercive powers and other direct action by the Government (for example, the declaration of a cyber security state of emergency, authorising the use of offensive powers), and oversight and review mechanisms. These matters are broadly relevant to questions 11, 19 and 28-24 in the Consultation Paper.[2]

5. In addition, as a general observation the Law Council notes that the proposed regime is likely to have a significant impact on business. The Law Council welcomes the general statement of intention in the Consultation Paper for the Government to 'ensure that the new requirements build on and do not duplicate existing regulatory frameworks'.[3] However, the Law Council considers that the development and release of a detailed Regulation Impact Statement (**RIS**) for the proposed regime should be released for public consultation, in advance of any legislation being introduced into Parliament.

6. The Law Council acknowledges the assistance of the Queensland Law Society in the preparation of this submission, and in particular its Privacy and Data Law Committee.

Key proposals requiring legislative amendments

7. The Consultation Paper provides limited detail about the proposed measures, particularly the nature of the governing legislative framework. On the Law Council's

[1] Department of Home Affairs, *Protecting Critical Infrastructure and Systems of National Significance: Consultation Paper*, (August 2020).

[2] Ibid, 30-31.

[3] Ibid, 12 and 17.

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

reading of the Consultation Paper, the key proposals that would require legislative amendments appear to be directed to the following matters:

- **an expanded regulatory regime**—the Consultation Paper appears to propose an expansion of the regulatory regimes in Part 14 of the *Telecommunications Act 1997* (Cth) and the *Security of Critical Infrastructure Act 2018* (Cth) to a wider range of critical infrastructure owners and operators, which would impose a positive, statutory security obligation on these entities to ensure the security of their infrastructure and associated systems and networks. It is unclear whether there is also a proposal to expand the mandatory information-disclosure obligations (and compulsory information-gathering powers) in existing legislation, so that owners and operators of covered infrastructure have an obligation to disclose certain information relevant to the security of their assets. It is also unclear whether there is a proposal to extend the current ministerial power of direction, under which the Minister for Home Affairs could issue legally binding directions to the owners or operators of a wide range of assets to take, or omit to take, certain actions in order to avoid causing prejudice to Australia's national security; and

- **a new emergency powers regime**—the Consultation Power appears to contemplate conferring a power on the Australia Government to declare a state of emergency with respect to cyber security, which would authorise the exercise of extraordinary powers ('offensive powers') to disrupt and respond to threats during the period of emergency.

Key rule of law principles for legislative and regulatory design

8. The Law Council acknowledges that an effective cyber security strategy, incorporating an efficient and effective regulatory framework, is critical in the current and projected future threat environment.[4] However, any legislative reform, including to emergency powers, must be consistent with fundamental principles underlying the rule of law.

9. It is particularly important to have clearly defined and commensurately rigorous frameworks, independent issuing and rights of review, and *ex post facto* independent oversight (by a single authority, or a federation of bodies with information-sharing and cooperative provisions to ensure appropriate coordination). Emergency powers must be strictly confined to a defined period of time that goes no further than is necessary to respond to an immediate or imminent threat.

10. The Law Council emphasises that these principles should be at the forefront of the design of any new or expanded regulatory regime, so that they are embedded in its fundamental design features from the outset.

11. This approach to legislative and regulatory design will go a considerable way towards ensuring that responses during emergency periods are measured and appropriate, and that major remedial amendments are not subsequently required during the Parliamentary scrutiny of the originating Bill, or in the later review of the regime once it is operational.

Effective legislative design principles and requirement of human rights compatibility

12. As a starting point in the design of the regime, the Law Council emphasises the importance of compliance with the established principles for sound legislative design, as set down and examined by the Senate Standing Committee for the Scrutiny of Bills and, so far as compatibility with human rights is concerned, mandated by the *Human Rights (Parliamentary Scrutiny Act 2011* (Cth) (**HR (PS) Act**) as applied by the Parliamentary

[4] Ibid, 6. See also: Australian Government, *Australia's Cyber Security Strategy 2020,* (August 2020), 10-14.

Joint Committee on Human Rights (**PJCHR**). The former set of principles requires compliance with a set of standards developed by the Senate Scrutiny of Bills Committee, while the HR (PS) Act requires an assessment of compatibility with Australia's international human rights treaty obligations, including those under the International Covenant on Civil and Political Rights.

13. In relation to human rights, there is considerable overlap between the two frameworks. In each case the proponent of legislation must show that if there is a potential to restrict human rights or to 'unduly trespass on personal rights and liberties', the proponent of legislation must demonstrate there is a legitimate purpose for doing so, a rational relationship between the goal and measures proposed, and that this is the least restrictive means of achieving the goal, as well as adequate mechanisms for independent review of decisions.[5]

14. The Scrutiny of Bills Committee requires proposed legislation to satisfy both rights standards as well as other principles of good legislative practice, namely:[6]

- **legislation should not unduly trespass on personal rights and liberties**—in particular, any limitation on human rights which can be permissibly limited must demonstrably be connected with a legitimate objective, and must be proportionate to the achievement of that objective. The Law Council cautions that the thresholds for exercising coercive and offensive powers should:

  - be subject to thresholds that explicitly require the decision-maker to be satisfied, on reasonable grounds, of the necessity and proportionality of the exercise of the power (including requirements for the decision-maker to consider impacts on all third parties, and a requirement to be satisfied that there is no less restrictive alternative that would be as effective in the circumstances);

  - wherever possible, be subject to consultation obligations as a pre-condition to the exercise of the power, or a contested application process by an independent decision-maker;

  - be subject to clearly defined time limits, periodic review requirements, and revocation and cessation obligations if the thresholds are no longer met;

  - ensure that issuing decisions are subject to independent review (ideally statutory judicial review) and *ex post facto* oversight;

  - include rights of compensation for loss, harm, injury or damage caused by the Commonwealth in the administration of the regime;

[5] The PJCHR has set out the applicable test as follows:

> *A measure that limits a right must be **prescribed by law**; be in pursuit of a **legitimate objective**; be **rationally connected** to its stated objective; and be a **proportionate** way to achieve that objective (the **limitation criteria**). These four criteria provide the analytical framework for the committee.*
>
> *A statement of compatibility for a measure limiting a right must provide a detailed and evidence-based assessment of the measure against the limitation criteria.*
>
> PJCHR, *Report 9 of 2020* (August 2020), vii (emphasis in original).

[6] See *Senate Standing Order* 24(1)(a). See further: Law Council of Australia, *Policy Statement: Rule of Law Principles*, (March 2011) which provides further detail on the implementation of the core scrutiny principles adopted by the Senate Standing Committee for the Scrutiny of Bills.

- be accompanied by a detailed RIS and privacy impact analysis (**PIA**). These documents should be released prior to the introduction of legislation.

- **administrative powers must be defined with sufficient precision, and delegations of legislative power must be appropriate**—in particular:

  - the prescription of the content of security obligations and the exercise of discretion about the exercise of coercive of offensive powers should be subject to prescribed and constrained legislative standards, and should not be dependent on the broad discretion of the relevant decision-maker; and

  - furthermore, if there is an intention to define the substance of sector-specific security obligations through the exercise of delegated legislative power to 'incorporate by reference' the contents of non-legislative instruments (such as industry codes of practice), that material should not be incorporated 'as in force from time-to-time'. Doing so would eliminate effective Parliamentary control, and potentially even visibility, over the content of the requirements;

- **appropriate review of decisions must be available**—in particular, the Law Council strongly supports the availability of statutory judicial and merits review of decisions to exercise coercive or offensive powers. The Law Council cautions that placing sole reliance on judicial review in the original jurisdiction of the High Court is likely to be inadequate in the case of decisions concerning matters of national security, given limitations in the applicant's ability to access necessary information to support their application;

- **any delegations of legislative power must be appropriate**—in particular, care should be taken to limit the proposed classes of any delegates to an appropriate level of seniority, skill and experience commensurate with the gravity of the power, including its direct and indirect impacts on third parties; and

- **the exercise of legislative powers must be subject to sufficient Parliamentary scrutiny**—the Law Council emphasises the importance of the legislative framework not leaving essential matters to delegated legislation, thereby reducing Parliamentary control over the regime. This should include the use of disallowable legislative instruments (this ensuring effective review by Parliament), and public and industry consultation in the development of such instruments (including with the national legal profession). There should also be appropriate arrangements for Parliamentary review of the regime, and public reporting on its use.

Safeguards and oversight measures

Authorisation of emergency powers

15. The Law Council submits that the threshold for prescribing a state of cyber emergency (or a similar concept of emergency that threatens to shut down or seriously disrupt the operation of critical infrastructure) must be set legislatively. That threshold must:

    - specifically prescribe the circumstances of 'emergency' that must exist in order for a declaration to be made. This should be by reference to the seriousness of the threat, including an assessment of its likely impacts, and its immediacy; and

    - explicitly incorporate criteria of necessity and proportionality, as pre-conditions to declaring a state of emergency and thereby enlivening emergency powers.

16. The Law Council considers that the power to declare a state of emergency must not be invested exclusively in a single Minister or other public official. While it may be necessary for an identified individual (perhaps the Governor-General-in-Council) to formally issue the instrument declaring a state of emergency, there must be statutory pre-conditions to ensure that such a declaration cannot be made in the absence of required consultation and advice, especially with States and Territories. In practice, this will require the involvement of State and Territory First Ministers, possibly through the National Cabinet or another forum.

17. Further, the Law Council emphases the need for national coordination in the exercise of emergency powers, and matters of day-to-day management during a state of emergency. Ideally, there should be an overarching federal body with such responsibility.

18. The Law Council further notes that, in State jurisdictions involving State owned assets, there will likely be constitutional issues which must also be considered in the legislative design and practical operation of the regime.

19. There will need to be cooperation between the federal body and the State agencies in this regard. It is always preferable for a transparent and consistent framework to be implemented across jurisdictions, as much as practicable where there are different State legislative requirements.

20. It is also important to ensure proper Parliamentary scrutiny of such declarations, including their continuing necessity. Such declarations (which should have a time-limited effect) may themselves be disallowable, but any declarations renewing them should eb subject to disallowance by Parliament.

21. The Law Council notes that the Senate Committee for the Scrutiny of Delegated Legislation is looking at these issues and recommends that the Government take into account the recommendations made by that Committee when it reports.

Independent oversight

22. The creation of any new powers and capabilities must be accompanied by proportionate safeguards and oversight measures. In particular, the Law Council supports the following measures:

- decisions concerning the issuing of mandatory directions should be subject to statutory judicial review, and declarations of a state of emergency should be subject to periodic review;

- the actions of all officials involved in the administration of the regime, including the exercise of coercive or offensive powers, should be subject to independent oversight, for example by the Commonwealth Ombudsman, the Inspector-General of Intelligence and Security, the Australian Commissioner for Law Enforcement Integrity, the Auditor-General and a Commonwealth Integrity Commission (when established). That oversight should be supported by the following measures:

  - appropriate notification and reporting mechanisms so that security agencies notify oversight bodies about the exercise of coercive and intrusive powers (including any offensive powers to disrupt cyber attacks), and powers of inspection. A specific inspection power will be necessary in the case of the Commonwealth Ombudsman, whose governing legislation does not include a general inspection power;

- appropriate resourcing to those agencies to perform their expanded oversight functions in relation to the new regime; and

- in the case of matters that involve multiple jurisdictions or multiple agencies subject to oversight by several different agencies, appropriate information-sharing provisions between oversight agencies, to support coordination of oversight activities (such as joint inquiries and inspections, and the sharing of relevant information obtained in their individual oversight activities).

23. The Law Council would also support the Independent National Security Legislation Monitor and the Parliamentary Joint Committee on Intelligence and Security being given specific oversight functions in relation to the new regime (with appropriate resourcing to perform these functions). This includes ongoing monitoring of the performance of functions and exercise of powers by relevant agencies or public officials, as well as a statutory review after the regime has been operational for a set period of time.

Other legislative and regulatory design issues

24. Feedback from the Law Council's membership has also identified the following matters, which should be reflected in the design and implementation of the regime.

- not all cyber-attacks, even if State sponsored, will have a uniform impact. The Government should develop a clear classification structure to assist critical infrastructure providers (**CIPs**) to identify when they should notify the Government of incidents, and when they should seek assistance;

- the regime should be supported by administrative guidance and training for all CIPs and government agencies to understand their respective roles in the operation and administration of the regime. The legislation should be sufficiently flexible to share information for these purposes, on a de-identified basis as appropriate to maintain privacy and security;

- the Consultation Paper appears to focus on CIPs generally, without specific consideration of small-to-medium enterprises (**SMEs**) that may be impacted by a cyber-attack. The Law Council supports specific attention being given to mechanisms for assisting SMEs, and the regulatory burden of any obligations imposed on them. These matters should be specifically addressed in the RIS accompanying the regime (which should, at the latest, be released as part of the Explanatory Memorandum to the Bill); and

- The Government should consider drawing upon relevant international materials, including the *Tallinn Manual 2.0*, which deals with the application of international law to cyber operations.[7]

Timeframes and process for the development of proposed legislation

25. Given the significance of the proposals and the limited details provided in the Consultation Paper, any measures proposed should be the subject of further public consultation in exposure draft legislation. The Law Council notes that this practice was extremely valuable in the development of the measures now contained in Part 14 of the *Telecommunications Act 1997* (Cth), with two rounds of exposure drafts provided for public consultation prior to the introduction of the amending legislation in 2017.

[7] Michael N Schmitt (General Editor), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (2nd ed), Cambridge University Press, (2017).

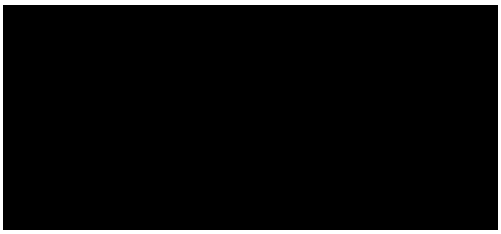
26. The Law Council understands from advice provided by officials of the Department of Home Affairs at its public information sessions on the Consultation Paper in August 2020 that there is no intention to release exposure draft legislation for the proposals, and there is an intention for a Bill to be introduced and passed in 2020.

27. The Law Council is concerned that the intended timeframe and consequent truncation of of pre-legislative consultations are not conducive to effective scrutiny of the proposed measures, which are likely to intrude significantly on business interests and individual rights and liberties. Moreover, the non-release of an exposure draft Bill may result in stakeholders, including the Law Council, raising a large number of issues during the Parliamentary scrutiny of a Bill, which could otherwise be addressed in pre-legislative consultations.

28. Accordingly, the Law Council urges the Government to reconsider the timeframes and process for the development of the proposed regulatory regime, particularly any proposal to confer 'offensive' powers of disruption on Commonwealth entities. The Law Council is able to draw upon industry and area specialists to assist in the commentary and recommendations on any draft legislation within tight but reasonable timeframes. Given the importance of the proposed legislation in this instance, the Law Council stands ready to review and assist in respect of exposure draft legislation in a timely manner, reflective of the importance and urgency of the subject.

29. Thank you for your consideration. The Law Council's nominated contact officer is listed on the electronic submission form covering this correspondence.

Yours sincerely



Pauline Wright
President