Joseph Lee
Barrister (ACT); Advocate & Solicitor (Malaysia)
LLB (Hons)(Tas) LLM by Research (Tas)
PhD Candidate (ANU)
[redacted]

The Hon Peter Dutton MP
Minister for Home Affairs
Parliament House
Canberra ACT 2600

16 September 2020

Dear Mr Dutton,

Protecting Critical Infrastructure and Systems of National Significance – Consultation Paper (August 2020)

Thank you for the opportunity to be part of the discussion on the proposed amendment to the *Security of Critical Infrastructure Act 2018* (SOCI Act).

I am a PhD candidate at the ANU College of Law. My thesis analyses Chinese corporations' investment in Australian critical infrastructure in order to provide recommendations on how the federal legislature can best secure Australia's national security through the regulation of the investment. The thesis analyses, among other legislation, the SOCI Act.

In this submission, I will address several questions posed by the Consultation Paper.

Q11. Do you think the security obligations strike the best balance between providing clear expectations and the ability to customise for sectoral needs?

In order to strike the best balance between providing clear expectations and the ability to meet sectoral needs, the SOCI Act needs to specify benchmark standards for discharging the proposed security obligations. A clear benchmark would help owners and operators to understand what is expected of them, and upon which regulators may assess their compliance with the proposed security obligations. In practice, owners and operators do have a strong vested interest to protect against all risks the critical infrastructure under their operations. The only question is: at what level should the obligations be discharged? Ideally, the required standards should be at the international level or accepted by the relevant sectors as best practice. This requirement should be stipulated in the SOCI Act rather than in the guidelines. This would avoid questions of its legal validity, and hence, enforceability.

A major hurdle to this recommendation is additional regulatory burden that carries increased cost for owners and operators. To cushion the negative impact of this, the federal government could provide financial incentives, such as a tax rebate for expenses incurred to meet the

proposed standards. While this would come at some cost to the Government, it would be a worthwhile investment to help achieve the objectives of the proposed amendment in the SOCI Act.

Q20 In the AusCheck scheme, potential and ongoing employees in the aviation, maritime, health and major national event security sectors undergo regular national security assessments by the Australian Security Intelligence Organisation and criminal history assessments to mitigate the risk of insider threats. How could this scheme or a similar model be useful in the sectors you are familiar with?

The AusCheck scheme could be both useful and burdensome. The scheme is helpful to mitigate insider risk as the checking system not only verifies the suitability of an employee to access critical infrastructure, but also puts that person who has satisfied the security checks on alert. The practical difficulty with this, however, is that employees who are subject to the screening process might submit an excessive number of documents to ASIO and the police, and this may prolong the verification process.

There is also the question of who should participate in the AusCheck scheme. One suggestion is to impose the requirement on all staff who are authorised to operate critical infrastructure. Another, the preferred choice, is that owners and operators nominate one single employee to undergo the security checks. The SOCI Act may subject this person to legal responsibility should insider risk materialise.

Q23 What information would you like to see shared with critical infrastructure by the Government? What benefits would you expect from greater sharing?

ASIO should share with the critical infrastructure sector the list of principles or criteria it uses to assess security risks. Currently, the critical infrastructure industry has no idea how and on what basis ASIO issues adverse national security assessments. This information would create certainty in the decision-making process of owners and operators, particularly in the area of risk management. Alternatively, the Government should share all unclassified information with the sector. Greater information sharing would enhance the cooperative relationship between the Government, owners and operators of critical infrastructure.

Q28 What safeguards or assurances would you expect to see for information provided to the Government?

Safeguards

i. The Government could implement a standardised receipt point to receive information that only falls within the scope of the SOCI Act;
ii. The computer system should only accept information that identifies specific individuals who are related to the cyber security threat.

Assurances

i. Sharing of information by the Government within its agencies should only be for limited purposes;
ii. The legislation must absolve individuals who supply the information to the Government of all civil and criminal liability, except for those stated in the SOCI Act.

Q36. Does this mix of obligations and assistance reflect the roles and responsibilities of the Government and industry in protecting critical infrastructure? How would the private sector's management of risk change with the proposed increased role for the Government?

The answer to the first part of the question is no. The TISN, Australia's Cyber Security Strategy, and the SOCI Act are predicated upon the principle of cooperation between the private sector and the Government in risk mitigation. The implementation of the proposed power may undermine the foundation and eliminate the mutual trust that has been built over many years. That said, in its current form the direction power in the SOCI Act is unable to satisfactorily address 'an immediate and serious cyber threat'. This is because the SOCI Act requires the Home Affairs Minister to consult Premiers and ministers in the state at which the critical infrastructure is located, as well as owners and operators in question; all of which may take a lengthy period of time. Instead of introducing the proposed power, the Government should amend the SOCI Act to cut short or expediate the consultation process.

Another issue emanating from the introduction of the proposed power is its potential duplication with the authority of state ministers under the *Essential Services Act* in New South Wales, South Australia, and Victoria. The state legislation authorises the relevant state ministers to command owners and operators to do or not do certain things. 'Emergency' is defined broadly in the state legislation to cover cases in which the supply of 'essential services' is or is likely to be disrupted or diminished. The only limitation of the state direction power is that it could not be invoked to alleviate all risks, particularly those unrelated to the supply of 'essential services', such as the threat of espionage. The Government has already addressed the loophole by introducing the direction power in the SOCI Act; albeit aimed specifically at addressing national security risks. It is therefore unnecessary to implement an additional power to allow the Minister of Home Affairs to intervene in cases that need urgent attention.

In relation to the second part of the question, the proposed power could drastically change the way owners and operators manage cyber security risks. In particular, they would need to take into account drastic intervention by the Home Affairs Minister. The recommended authority would add uncertainty to their mitigation plan and business operations more generally. More worrying is the element of fear the proposed power would generate. Owners and operators may conduct their business under constant anxiety the Government could intervene at any time if it disagrees with the way they manage cyber security risks. In the long run, this would not help to promote Australia as a preferred destination for foreign investment in critical infrastructure.

Yours sincerely,
Joseph Lee