Dr Michael Spence AC
Vice-Chancellor and Principal

27 November 2020

Department of Home Affairs
Canberra

Submitted via https://www.homeaffairs.gov.au/reports-and-publications/submissions-and-discussion-papers/protecting-critical-infrastructure-systems/submission-form

Protecting critical infrastructure and systems of national significance
Exposure Draft of the Security Legislation Amendment (Critical Infrastructure) Bill 2020 (Cth)

Thank you for the opportunity to provide the attached feedback on the Exposure Draft of the *Security Legislation Amendment (Critical Infrastructure) Bill 2020 (Cth)*.

We have contributed to and endorse the submissions from Universities Australia and the Group of Eight and provide this submission to complement the feedback they have provided on our behalf.

The University of Sydney supports the national security policy objectives that underpin the proposed amendments to the *Security of Critical Infrastructure Act 2018 (Cth)*, including the proposed expansion of the Act's coverage to apply to assets in the higher education and research sector.

It is vital that critical infrastructure (facilities essential for everyday life such as energy, food, water, transport, communications, education, research, health, banking and finance) is protected. However, a proportionate and workable regulatory approach is required. This includes a tighter definition for a 'critical infrastructure asset' owned and operated by a higher education provider, to ensure that the proposed protection regime applies only to assets that, if compromised, would represent a threat to the nation.

Further work is needed to quantify the likely additional compliance costs that these proposed changes will impose, particularly for public research-intensive universities determined to be responsible for critical infrastructure assets deemed to be 'Systems of National Significance'.

We share the concerns our peak bodies and others have expressed about aspects of the proposed civil liability provisions as well as the exclusion of decisions from administrative review under the *Administrative Decisions (Judicial Review) Act 1977 (Cth).*

Thank you again for this opportunity and we trust that this feedback is helpful. Should the Department require anything further from the University, please do not hesitate to contact Mr Tim Payne, Director, Higher Education Policy and Projects, Office of the Vice-Chancellor and Principal ([redacted], [redacted]).

Yours sincerely,

[redacted]

Michael Spence

Office of the Vice-Chancellor and Principal
F23 - Administration Building
The University of Sydney
NSW 2006 Australia

T +61 2 9351 6980
E vice.chancellor@sydney.edu.au
sydney.edu.au

ABN 15 211 513 464
CRICOS 00026A

The University of Sydney, feedback on the Exposure Draft of the Security Legislation Amendment (Critical Infrastructure) Bill 2020

1. Compliance burden and associated costs

The amendments proposed in the Exposure Draft are extensive and would impose significant obligations on public universities declared by the Minister to own or operate a 'Critical Infrastructure Asset'. Even more significant obligations would be imposed on a university declared to own or operate one or more assets designated as a 'System of National Significance'. We note, for example, the possible requirement to install and maintain a computer program capable of harvesting the system information relevant to the computer operating such systems (including cleansing it of personal information) for transmission to the Australian Signals Directorate.

Universities affected by a rule or determination of the Minister will become subject to an additional regulator. The regulatory obligations will be extensive and costly in terms of the resourcing required to support compliance with the regime. While we understand and support the policy objectives underpinning the Bill, we are concerned about the likely additional compliance costs for public universities responsible for operating critical national research infrastructure – often effectively on behalf of the Commonwealth and in some cases in collaboration with Commonwealth research agencies, state or territory government entities and other universities.

2. The Minister's rule making powers

The Exposure Draft gives considerable powers to the Minister to make rules and determinations which implement the broad objectives of the legislation. While the Bill does, in numerous instances, indicate one or two factors the Minister must consider when making rules and determinations, the factors are few and widely drawn. This results in the Minister having little substantive legislative guidance but substantial powers. For example, only one factor is cited in assessing whether or not to declare a Critical Infrastructure Asset to be a 'System of National Significance'.

The absence of relevant factors to guide the Minister in his or her rule making is of concern as it impacts the basis on which any rule making can be reviewed.

Additionally, we would appreciate sector-wide consultation with the Minister's representative, which would allow universities to understand the intended reach of the rule making powers of the Minister before the Rules are released. This is important given the absence of review mechanisms for some of the powers included in the Exposure Draft.

3. Reporting

The Exposure Draft proposes significant reporting obligations for entities responsible for assets covered by the legislation, imposing cost and requirements for additional resources. Moreover, many of the provisions attract civil penalties for failure, inadequate or incomplete performance. Additionally, prevention activities, reporting of and mitigation of cyber security events (set out in Part 2B of the Exposure Draft) are to be delivered in very short time frames. Having the relevant infrastructure in place to enable fast turnarounds in reporting will come at a significant cost at a time when universities have been impacted by the coronavirus, decline in international student attendance and associated student income, the costs of delivering remote learning and keeping campuses open during a pandemic and associated factors.

We also note the proposal for substantial civil penalties to apply for failure to meet reporting obligations, including failure to use the prescribed form or inadequate use of the prescribed form 30BE (4). The other issue of concern is the point at which an obligation to report a cyber security incident arises.

The Bill repeats the problem that has appeared in data breach notification provisions in various privacy legislation. The obligation arises when the entity becomes 'aware' of an incident. **The time at which an entity becomes 'aware' of a breach has been the subject of very different interpretations in the data breach notification regimes and should not be taken at face value. We would be happy to work with the Government and affected sectors to develop a workable definition.**

4. Enhanced cyber security obligations

The layer of more onerous cyber security obligations set out in Part 2C 'Enhanced Cyber Security Obligations' (where a declaration has been made as to 'Systems of National Significance') does not place any parameters around the information the system reporting software is required to produce. Further guidance should be included to establish clear expectations about the information that must be collected and reported. The parameters for the 'Intervention Request' would also benefit from the inclusion of more clearly defined limitations. As proposed in the Bill, the Australian Signals Directorate can access and remove computers; copy, analyse and modify data; and alter the function of a computer. This represents quite an extreme approach, which could undermine an entity's autonomy over its systems. **For entities and the community to have confidence that this power will be exercised appropriately, the legislation should specify the type and severity of an event that would entitle the Directorate to invoke such a power.**

5. Civil liability

The many penalties imposed under the Exposure Draft are civil and not criminal. However, in respect of 'Systems of National Significance', we note that individuals who would normally be able to claim a privilege against self-incrimination are not excused from providing a report under section 30DB, should the report tend to incriminate the individual (s30DG Self-incrimination).
The right to avoid self-incrimination is fundamental to a society based on the rule of law. It should not be removed by legislative provisions attempting incursion into normal criminal protections.

6. Review

The Exposure Draft contains the usual provisions for departmental review of the Rules with the Minister having to make a statement of findings within 15 days of receipt of the report from the Department. **However, no mechanism is provided for independent review of the operation of the legislation. We suggest that this be encouraged through a steering committee, or similar, comprising experts with relevant security clearances able to represent their sectors. The committee could meet twice a year to discuss issues arising from implementation of the new legislation**.

7. Administrative Decisions (Judicial Review) Act 1977

Decisions under Part 3A of the *Security of Critical Infrastructure Act 2018* are not subject to review under the *Administrative Decisions (Judicial Review) Act 1977*. Part 3A of the Exposure Draft deals with *responding to serious cyber security incidents*. **We do not support the exclusion of a right of review, which is a basic right in any society held together by the rule of law**.

8. Health care and medical sector

It is possible that a university may be considered, in certain circumstances, to be part of the health care and medical sector (for example, in circumstances where an employee of a university is delivering health care in a university clinic within a public hospital facility or is jointly employed with a health service or medical research institute to operate research infrastructure or facilities) and we think that effect would be unintended. **We support clarification that it is not intended that universities should straddle other sectors in addition to the higher education and research sector.**

Ends/