Professor Mark Scott AO
Vice-Chancellor and Principal

31 January 2022

The Hon Karen Andrews MP
Minister for Home Affairs
Department of Home Affairs

Via email: CI.Reforms@homeaffairs.gov.au

Dear Minister Andrews,

Exposure Draft of the Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022

Thank you for the opportunity to comment on the exposure draft of the *Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022*.

We provide this feedback to complement the submissions being made by the Group of Eight and Universities Australia on behalf of their member institutions and acknowledge the series of town hall sessions that your Department has hosted to provide information to the sectors affected by the new and proposed legislation.

The University of Sydney supports the national security policy objectives that underpin the amendments already made to the *Security of Critical Infrastructure Act 2018* (Cth). However, we would like to raise the following points regarding the exposure draft of the new Bill:

1. The definition of Higher Education and Research is not sufficiently clear, to indicate which institutions within the sector fall within its scope and which activities and facilities at those universities are within scope. We do not want to be in a position of having to confirm with the Department which activities/facilities are in or out of scope. We also do not think it helpful to propose an alternative definition, as the Commonwealth is best placed to communicate the intended reach of the legislation.

2. The mechanism for diverting some sectors to their own risk management framework needs to be reflected more clearly in the legislation so that there is a transparent procedure through which members of the sector know they are being compliant. In the case of universities, the Department has advised that compliance with a University Foreign Interference Taskforce (UFIT) risk management framework, as supported by the *Guidelines to counter foreign interference in the Australian university sector*, will be sufficient to comply with the Act. Each institution requires certainty that they are compliant with the Act and not subject to penalty if that university's framework does not mirror each and every provision set out in the Act.

3. There is a concern that the application of the cyber security provisions will not be sufficiently well understood unless and until the Australian Cyber Security Centre's (ACSC) Guidance is available and can be discussed with the ACSC. There is a lack of

Office of the Vice-Chancellor and Principal
Level 4, F23 The Michael Spence 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

clarity about how the ACSC Guidance can be accessed; and if it is general in nature, sector-specific or tailored to the institution. The University would appreciate knowing when engagement with the ACSC is expected to commence and how that guidance will be delivered. For example, the Exposure Draft describes certain types of cyber security incidents that are reportable. You would appreciate that at the current time the University receives daily threats, which range in severity and complexity but are mitigated by our cyber security team. It is unclear whether such incidents (dealt with by the University as part of business-as-usual for our cyber security team) will need to be reported. It would be helpful if the Commonwealth could describe the type, intensity and duration of the types of incidents that trigger one of the several reporting obligations.

4. The reporting and turnaround period of 30 days in respect of section 30CZ(b)(i) is short, in respect of the information that needs to be gathered. We would appreciate it if greater flexibility was provided, say up to a period of 45 days if necessary.

5. We find the description of cyber security incidents as “significant” or “critical” without further explanation to be an unhelpful classification. It would be helpful if the legislation referenced those areas of the guidance that provide more detailed explanation.

6. We appreciate the wide-reaching, regular and timely consultation that has taken place and the flexibility with which it has been delivered during this period of remote working. The consultation phase has uncovered numerous sector-specific issues and the University is of the view that these will continue to emerge during the implementation period as the legislation is tested against real-world experience. We again suggest that there would be great utility in having an overarching steering group providing feedback to you on the effectiveness of the implementation and any issues arising for a period after commencement of the amending Act. Underneath that steering group could be 11 sector groups, confined in size, which would provide feedback to the overarching steering group on the operation of the Act and rules in their sector, including any challenges.

Finally, as noted in previous submissions, we are concerned about the cost of compliance with the cyber security requirements. While we understand and support the policy objectives underpinning the security of critical infrastructure legislation, we remain concerned about the likely impost for public universities of these additional compliance measures.

Thank you again for this opportunity to comment – we trust that this feedback is helpful.

Yours sincerely,

Mark Scott

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