Professor Mark Scott AO
Vice-Chancellor and Principal

1 February 2022

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

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

Dear Minister Andrews,

Security of Critical Infrastructure (Application) Rules 2021
Mandatory cyber incident reporting for critical infrastructure assets

We refer to correspondence from the Department of Home Affairs notifying the University of Sydney that we have been identified as an asset which you intend to specify in rules or a declaration made in accordance with paragraph 30BBA(2)(d) of the *Security of Critical Infrastructure Act 2018*, as amended by the *Security Legislation Amendment (Critical Infrastructure) Act 2021*. The letter from your Department was accompanied by the explanatory statement on the Security of Critical Infrastructure (Application) Rules 2021 (Rules).

Thank you for the opportunity to comment on the draft Rules. We are providing this feedback to complement the submissions being made by the Group of Eight and Universities Australia; to which we have also contributed our views.

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

1. The reporting and turn-around 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 if greater flexibility was provided, say up to a period of 45 days if necessary.

2. 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 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.

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

3. 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 Australian Cyber Security Centre’s (ACSC) Guidance that provide more detailed explanation.

4. It is not abundantly clear from reviewing the draft rules and legislation that public universities will be exempt from complying with the Risk Management Program and that, instead, risk management requirements and reporting for universities will be dealt with through a University Foreign Interference Taskforce (UFIT) risk management framework, as supported by the *Guidelines to counter foreign interference in the Australian university sector*.

5. There is a concern that the application of the cyber security provisions will not be sufficiently well understood unless and until the ACSC Guidance is available and can be discussed with the centre. There is a lack of clarity about how that guidance can be accessed; 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 that 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 the University 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.

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

Yours sincerely,

(signature removed)

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