Universities Australia's response to the Cyber Security Legislative Package 2024 inquiry

25 October 2024

Introduction

Universities Australia (UA) welcomes the opportunity to make a submission to the Parliamentary Joint Committee on Intelligence and Security's Review of the Cyber Security Legislative Package 2024. UA is the peak body for Australia's 39 comprehensive universities, each with a strong interest in the enhancement of cyber security protection in Australia. Many of our members have expertise in cyber security, having contributed to the *2023-2030 Australian Cyber Security Strategy* consultation.

Australian universities are highly engaged with the issue of cyber security, providing inputs into, and sharing best practices on cyber security with, forums including the University Foreign Interference Taskforce (UFIT), the Council of Australasian University Directors of Information Technology (CAUDIT), the Australasian Higher Education Cybersecurity Service (AHECS), the Trusted Information Sharing Network (TISN) and the Enhancing Cyber Security Across Australia's University Sector Project delivered by RMIT. This has led to a significant increase in awareness and responsiveness to cyber security issues across the sector, and a maturation of threat modelling, policies, procedures, and governance within our universities.

Many of our members are responsible for critical infrastructure assets under the *Security of Critical Infrastructure Act 2018* (SOCI Act). Continued engagement within the sector and with government has ensured that obligations under the SOCI Act have been comprehensively met, although there are areas of this legislation that lack definitional and operation clarity.

UA is broadly supportive of the legislative package but has some concerns around increased reporting obligations and duplicative requirements for universities. The key points presented below are provided to the Committee to detail the impact the additions to the legislative framework surrounding cyber security will have on universities from a regulatory burden perspective, as well as suggesting additional enhancements that we believe will strengthen the framework.

Mandatory reporting for ransomware and additional reporting obligations

The measures introduced in the *Cyber Security Bill 2024* address issues raised in the *2023-2030 Australian Cyber Security Strategy* and in subsequent consultation. The introduction of mandatory reporting for ransomware, including an additional reporting obligation for entities that are both reporting business entities and responsible for a critical infrastructure, appears to be duplicative without providing additional benefit. The explanatory memorandum indicates that "enlivening the ransomware reporting obligation will ensure there is a complimentary reporting framework in place to capture reports that are required to be made under existing provisions within the SOCI Act" but gives no indication of how complimentary reporting frameworks will operate in conjunction with these provisions.

The additional reporting obligation suggested by this legislative package adds to an already extensive and multifaceted cyber security reporting environment. Our members have identified the Australian Signals Directorate's (ASD) Australian Cyber Security Centre

(ACSC), the Office of the Australian Information Commissioner, UFIT, and state-based organisations as requiring contemporaneous reporting of cyber incidents.

Consideration should be given to how reporting requirements can be further aligned. This could be achieved by merging the reporting platform intended for the *Cyber Security Bill 2024* with the existing ASD ACSC platform used for SOCI Act reporting. This would remove duplicative reporting requirements, facilitating coordinated responses from responsible government entities such as the National Cyber Security Coordinator and the proposed Cyber Incident Review Board. Streamlined reporting is highlighted in the *2023-2030 Australian Cyber Security Strategy* as an area for improvement, which should be further clarified beyond what is included in this legislative package.

Additional enhancements to cyber security incident reporting could include allowing for updates to existing reports when new information arises, providing a record of information submitted, and a comprehensive review of existing government reporting mechanisms to determine where information is being duplicated.

Cyber Incident Review Board

UA supports the establishment of a Cyber Incident Review Board to conduct post-incident reviews, and provide recommendations around prevention, detection, response and minimisation. The Cyber Incident Review Board and Expert Panel should operate independently, with transparent appointments and membership.

The positioning of the National Cyber Security Coordinator and Cyber Incident Review Board as whole of government responders is welcomed given the complexity of existing reporting obligations discussed above. Through the operation of these entities, it is anticipated that efficiencies will be identified from a government-response perspective that could lead to greater interoperability of cyber incident reporting. This is a desirable outcome for both universities and government as reduced regulatory burden and reporting complexities will allow for cyber security incidents to be managed more expeditiously.

The role of universities in developing cyber security capabilities

There is considerable cyber security expertise within Australian universities that should be utilised in the implementation of this legislative package. In particular, the Expert Panel component of the proposed Cyber Incident Review Board should draw on the expertise of the sector.

A non-exhaustive list of cyber security centres in our membership includes; the RMIT Centre for Cyber Security Research and Innovation, the Academic Centres of Cyber Security Excellence, the Edith Cowan University Centre for Securing Digital Futures, the Deakin Cyber Research and Innovation Centre, UQ Cyber, Macquarie University Cyber Security Hub, the University of Wollongong Institute of Cybersecurity and Cryptology, the UNSW Institute for Cyber Security, the James Cook Cyber Security Hub, and the Cyber Security Cooperative Research Centre.

Government agencies should continue to communicate and engage with universities on the implementation of this legislative package to ensure sufficient guidance is given. This has been managed through forums such as UFIT and TISN, which are valuable sources of information on cyber security best practice, however further clarity around ambiguous or generalised requirements is needed. In particular, universities will need to be supported to implement amendments to data storage requirements within the SOCI Act, which continue to contain non-specific definitions and requirements.