GROUP OF EIGHT AUSTRALIA

**The Group of Eight Limited**
ABN 98 089 687 990

GPO Box 139
Canberra ACT 2601
Level 4, 10 Moore Street
Canberra ACT 2600
Australia

**t: +61 (0)2 5123 6700**
**www.go8.edu.au**

24 October 2024

Senator Raph Ciccone
Parliamentary Joint Committee on Intelligence and Security
c/o Committee Secretary
PO Box 6021
Parliament House Canberra ACT 2600
Email: pjcis@aph.gov.au

Dear Senator Ciccone

**Go8 submission on the Review of the Cyber Security Legislative Package 2024**

The Group of Eight (Go8) is pleased to provide this submission to the Parliamentary Joint Committee on Intelligence and Security Review of the Cyber Security Legislative Package 2024. Please note this submission represents the views of the Go8 network, and member universities may choose to make their own submissions.

The Go8 remains committed to Australia becoming a leading cyber secure and resilient nation and to safeguarding our university assets, digital networks and environments including as a basis to building trusted domestic and global relationships.

The Go8 worked collaboratively with the Government in the development of the important reforms that saw the higher education and research sector added in 2021 to sectors regulated by the Security of Critical Infrastructure Act 2018 (SOCI Act 2018). The Go8 supported recognition that a critical education asset cannot wholescale include all assets within the university, with a final definition narrowing the scope to focus on research. The Go8's input, as well as input regarding the critical education asset, was also reflected in the exemption from certain Positive Security Obligations under the SOCI Act 2018, namely registration of assets on the critical infrastructure register and the requirement for risk management programs.

These nuanced changes were arrived at after a prolonged set of discussions, which included the Go8's representations to the Committee at its Review of the proposed changes to the SOCI Act in 2021 and 2022[1], and demonstrated the value of a genuine and deliberative consultative approach.

**Notwithstanding this, Go8 universities experience significant regulatory burden as a result of the SOCI Act, and the Go8 would urge that these additional reforms must judiciously balance the imperative for reform and the resulting impost on regulated entities. The new reforms warrant as careful a design process as those in 2021/2022 if they are to be effective.**

[1] This included the PJCIS review of the Security Legislation Amendment (Critical Infrastructure) Bill 2020 and Statutory Review of the Security of Critical Infrastructure Act 2018; and its Review of the Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022.

The Go8 makes the following recommendations to the Committee:

1. That the Committee emphasise in its review **the need for the proposed reforms to limit unnecessary regulatory burden or government intervention and for those reforms to work harmoniously with existing regulatory requirements** including those already existing under the Security of Critical Infrastructure Act 2018 (SOCI Act) and privacy legislation.
    a. Consideration should be given to whether requirements introduced for ransomware reporting occur under the SOCI Act 2018 for those sectors already subject to that Act, rather than as proposed under the eventual Cyber Security Act.
2. That the Committee **support the threshold proposed for the reporting of ransomware attacks. i.e.** a payment or benefit must have been made to the perpetrator of the related cyber security incident.
3. That the Committee recommend that **further precision and tightening up of key terms and threshold issues** to increase the efficiency and likely success of the reforms, as well as reduce the regulatory burden on regulated entities.
4. That the Committee seek **a refined design of the proposed expanded all hazard 'consequence management' power**, that considers that the current approach to cyber security incidents cannot simply be duplicated in relation to non-cyber incidents.
5. That the Committee **endorse the limitation of the expanded all hazard 'consequence management' power for non-cyber incidents to a power to seek information and direct action, and preferably at the request of the impacted entity**, but not to intervene as authorised for cyber security incidents.
6. That the Committee endorse the intent for the proposed Cyber Incident Review Board's **expert panels to be drawn from a pool of industry experts with high levels of cyber security, legal or sectoral expertise and experience**.
7. That the Committee **support the intent to limit use of information** gathered by Government including the Australian Signals Directorate (ASD), the National Cyber Security Coordinator and other agencies or by the Cyber Incident Review Board.

***General***

The Go8 recognises the heightened risks arising from an increased prevalence and sophistication of cyber security threats and supports the ongoing need for readiness and vigilance to enable response to or prevention of related incidents. There is no lack of willingness of Go8 institutions to comply with existing requirements nor to voluntarily share relevant information without breaching other legal obligations with regulators such as the Australian Signals Directorate (ASD) and the National Cyber Security Coordinator.

Nevertheless, as noted in Go8 submissions to the Department of Home Affairs this year, the regulatory impost on universities as regulated entities is significant and arises at least in part due to uncertainty regarding the meaning and appropriate interpretation of key elements of the Act. As a result:

- There can be an abundance of caution in compliance approaches, to ensure that nothing is inadvertently missed, and this comes at a cost to universities.
- Multiple areas and teams may need to work in conjunction to ensure compliance, which is not a simple undertaking in a large institution.
- There can be the potential for misinterpretation of those terms that have a potentially wide breadth of possible meaning or application, and vary from sector to sector, such as business critical data.
- Identification and management of relevant assets can be challenging and time consuming in a research-intensive university.

GROUP OF EIGHT AUSTRALIA

***Need to limit unnecessary regulatory burden or government intervention and for those reforms to work harmoniously with existing regulatory requirements***

In response to the statement in the explanatory memorandum to the Security of Critical Infrastructure and Other Legislation Amendment (Enhanced Response and Prevention) Bill 2024 **that the higher education and research sector (along with several other sectors) either did not provide cost estimates** for proposed measures or were unable to do so, we reiterate that it is not possible for individual institutions or the sector to readily quantify the regulatory costs.

However, qualitative indications such as noted above go to rebutting any assumption that there will not be a material impact on costs for the higher education and research sector – as noted in our submission on the impact analysis to the Department of Home Affairs in March. The Go8 rejects any assumption that the new requirements will not result in significant regulatory costs for the university sector, which are not subsidised by the Government.

- This is of particular concern as the sector anticipates significant defunding due to international student caps being proposed by the Government. As noted in our March submissions, the costs of supporting effective and efficient solutions to enable compliance are likely to be considerable.

The addition of new regulatory measures, however necessary, is likely to exacerbate the burden, and we would urge the Committee to consider that in terms of impact **these reforms are potentially as significant for universities as those that brought the sector under the purview of the SOCI Act 2018. The proposed legislative changes therefore need to be as refined and tailored as possible, to reduce the potential for confusion and inadvertent overreach.**

- As an example, we note that key university data can primarily be personal information that is already regulated and subject to mandatory reporting obligations under several pieces of privacy legislation including state-based legislation. Such data can be business-critical data and would at least meet the aspect of the definition in the SOCI Act on 'information relating to at least 20,000 individuals', which is easily reached in institutions of the size of Go8 universities.
- Yet there is some confusion caused by the statement in the explanatory memorandum that while data storage systems can hold personal information and other 'business critical data', it is not expected that personal information would be impacted by the amendments as they will only relate to data storage systems where there is a material risk that a hazard to that system would have a relevant impact on the functioning of the critical infrastructure asset[2].
- There is the need for greater clarity in this respect as well as delineation of SOCI Act obligations versus other (e.g. privacy obligations).

Reporting obligations in relation to ransomware

On a specific matter, the Go8 had recommended to the Department of Home Affairs that those sectors regulated by the SOCI Act 2018 – and already reporting under that Act – would ideally report under that Act when it came to ransomware reporting requirements.

[2] P.92 of the EM to the Security of Critical Infrastructure and Other Legislation Amendment (Enhanced Response and Prevention) Bill 2024

It remains unclear why ransomware incident reporting would need to occur under a separate legislative regime than the SOCI Act 2018 which regulates the reporting of other cyber security incidents under Part 2B.

While the Go8 welcomes advice from the explanatory memorandum for the Cyber Security Bill that entities would report on ransomware incidents via the ASD's Australian Cyber Security Centre (ACSC) reporting portal, similarly to reporting cyber security incidents currently, there is scope for confusion and additional impost for regulated entities who would need to understand the Cyber Security Act as well as the SOCI Act 2018.

The Go8 supports the threshold proposed for the reporting of ransomware attacks, that is that a payment or benefit must have been made to the perpetrator of the related cyber security incident, and would urge the Committee to recommend that this feature be retained in the final legislation.

**Further precision and tightening up of key terms and threshold issues**

Go8 members have noted that difficulties in complying with the SOCI Act stem from a lack of definitional clarity and that there should be further guidance or qualification of major elements, including underpinning criteria regarding what the reforms would aim to protect. This would reduce unnecessary organisational impact of the proposed reforms.

Given the increased significance of **'business critical data'** as the basis for triggering obligations in relation to data storage, including that related to secondary **'non-operational' data storage** systems, there would be benefit in further explanation and characterisation of what could constitute such data, beyond the definition in the current SOCI Act.

Other key terms that warrant specific definition, further explanation or contextual advice include but are not limited to material risk, data storage and serious incident (which demands a threshold of what constitutes seriousness). It would also be helpful to have a better understanding of relevant terms such as manufacturer and supply in the case of smart devices.

**Refined design needed of the proposed all hazards 'consequence management' power**

The proposed all hazards 'consequence management' power intended under the Security of Critical Infrastructure and Other Legislation Amendment (Enhanced Response and Prevention) Bill 2024 requires further design and explanation.

The Go8 welcomes the intent that intervention **requests are to be limited to cyber security incidents and seeks that the Committee support this intent**.

Clearer rationale

**Clearer rationale** – beyond the examples provided – would assist in understanding the proposed extension of the Minister's power in two directions: to manage consequences of an incident, and to cover all hazards (including and in addition to cyber).

- The example given of research data stolen from a university is specifically a cyber incident, as discussed in the 2021-22 reforms, and does not add much context for the higher education and research sector.

- Other examples, such as gas pipeline sabotage and heavy flooding impacting a critical asset, are illustrative but not sufficient context.

'Serious incident'

Advice is needed on the threshold for what would be considered a **'serious incident'** as the replacing phrase for 'serious cyber security incident'.

- The term is qualified in the bill as a *'serious incident that has had, is having, or is likely to have, one or more relevant impacts on one or more critical infrastructure assets'*. However, this provides no further clarity even considering the meaning of **relevant impact**, which goes to availability, integrity, reliability or confidentiality of the asset.
- The explanatory memorandum (para 50) notes *'"serious incident"* is an undefined term in the SOCI Act and is intended to take on its ordinary meaning'.

Consideration should be given to **aligning 'seriousness' with the criteria proposed as the threshold for when the Cyber Incident Review Board review an incident**, being those that:

- have seriously prejudiced or could reasonably be expected to seriously prejudice the social or economic stability of Australia or its people, or the defence of Australia, or national security. (It is interesting to note that serious prejudice is additionally explained in the explanatory memorandum).
- involved novel or complex methods or technologies and by undertaking the review, the understanding and recommendations made will result in being able to significantly improve Australia's preparedness, resilience, or response to (cyber) security incidents of a similar nature
- that are, or could reasonably be expected to be, of serious concern to the Australian people.

'Multi-asset incidents'

Further qualification may also be needed as to whether the power is intended to chiefly deal with management of **'multi-asset incidents'**, a term used in the explanatory memorandum (paragraph 38) but not in the bill.

Impacts, ramifications and expected directions

Further refinement would also be useful regarding **the actual expected impacts or ramifications of the extended consequence management powers**.

- Clarification is essential regarding the likely action request that Government will ask of the entity in the case of non-cyber security incidents. The example in the SOCI Act 2018 (12P) currently of an action being to seek the 'Restoring the functioning of the asset' may be appropriate if dealing with cyber security incidents and cyber/digital/computer elements of that asset, but not if dealing with a major natural event and impact on physical infrastructure whose function may not be restorable. Given the penalty may be two years imprisonment or 120 penalty points or both, regulated entities should be provided further detail regarding what to expect in such a circumstance.
- It is also unstated as to what powers are in play if a non-cyber hazard results in a cyber security incident.

GROUP OF EIGHT AUSTRALIA

**Cyber Incident Review Board**

The Go8 welcomes the detail provided – which we advocated for as a preliminary step to determining whether an existing or new separate body is needed – on the functions and purpose of the proposed Cyber Incident Review Board.

While the Go8 does not deny the value of retrospective reviews of major cyber incidents and welcomes the intent for the Board to be independent, there is a remaining question as to whether those functions can be undertaken by an existing independent body.

Further, it is not clear how the Board would interact with existing bodies such as the Executive Cyber Council, on which clarification would be useful as the Board is formed.

Clear delineation of responsibilities between **the Minister and the Board is needed** if the Board is to indeed be independent. Despite the intended independence, the bill proposes that the Minister play a major role including in appointing Board members and the Chair, agreeing terms of reference for reviews, and receiving draft review reports on which the Minister may provide a submission to the Board.

- The Board could also be used as a mechanism to review the Government's own response to a cyber security incident when the Government has wielded assistance powers.

The Go8 supports the intent for the proposed Cyber Incident Review Board's expert panels to be drawn from a pool of industry experts with high levels of cyber security, legal or sectoral expertise and experience, and we would be pleased to advise details of such individual experts from Go8 universities.

Other

The Go8 strongly supports the intent to prescribe and limit the use of information shared with the Government, including in relation to protected information, ransomware reporting information, information shared with ASD and regulated under the Intelligence Services Act, as well as information sought by and shared with the Cyber Incident Review Board.

Thank you for the opportunity to provide this submission.

Yours sincerely,

[redacted]

**VICKI THOMSON**
**CHIEF EXECUTIVE**