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

1 March 2024

Department of Home Affairs
Submission via web portal

Go8 response to the Australian Government's 2023-2030 Australian Cyber Security Strategy: Cyber Security Legislative Reforms Consultation Paper

The Group of Eight (Go8) welcomes the opportunity to provide this submission to the Australian Government's Cyber Security Legislative Reforms Consultation. Please note this submission represents the views of the Go8 network, and member universities may choose to make their own submissions.

The Go8 consents for this submission to be published in full.

The Go8 has consistently recognised the importance of Australia becoming a leading cyber secure and resilient nation. We acknowledge the criticality of safeguarding our university assets, digital networks and environments to building trusted domestic and global relationships.

Given that our leading research-intensive universities are engaged in global education and research collaboration, Go8 universities take a responsible and diligent approach to ensuring our institutional and shared cyber security. Our members have engaged readily with the obligations created by the expansion of the Security of Critical Infrastructure Act 2012 (SOCI Act) to the higher education and research sector and to education assets. While we question assumptions that universities are more vulnerable and susceptible to attack than other Australian sectors, our universities have nevertheless built a stronger culture of security, recognising that major geopolitical shifts have exposed Australia to greater cyber risk.

Recommendations

1. The proposed reforms must not introduce unnecessary regulatory burden or government intervention and should work harmoniously with existing regulatory requirements including the Security of Critical Infrastructure Act 2018 (SOCI Act), privacy and data-sharing legislation.
    a. A specific recommendation is that requirements introduced for ransomware reporting should occur under the SOCI Act for those sectors already subject to that Act, rather than under a separate legislative instrument.
2. Key elements of proposed reform need to be clearly defined, including but not limited to 'business critical data', 'material risk', 'data storage systems', and thresholds for Government intervention, to limit misinterpretation and costly or ineffective implementation of reforms.
3. Any requirements for affected entities arising from the proposed limited use obligation for ASD and the NCSC to encourage engagement by industry following a cyber incident, should be aligned with existing requirements, including under the SOCI Act.
4. Government intervention in relation to consequences of significant incidents should be a last resort, or at the explicit request of the relevant entity.
5. The functions of the proposed Cyber Incident Review Board should be clearly established in advance of determining the need for such a body, and once defined guide the decision as to how the functions could be carried out and whether an existing body can implement these.

Discussion

RECOMMENDATION 1

Design of reforms should have due regard to where and how proposed new regulatory requirements can be pursued through existing Federal legislative or other mechanisms, such as the Security of Critical Infrastructure Act 2018 (SOCI Act), the Privacy Act 1988, the Data Availability and Transparency Act, and have due regard to the reforms working in concert with existing relevant federal and state legislation (including privacy and data sharing).

For those sectors and entities regulated by the SOCI Act, reporting of ransomware incidents (Measure 2) should occur under that regime. This would prevent the onerous addition of a separate reporting mechanism. For those sectors regulated by the SOCI Act, it would be more cost-effective to apply and enforce the existing SOCI Act reporting requirements. The Consultation Paper estimates that approximately 1000 Australian entities fall under the SOCI Act's mandatory reporting obligations that require the reporting of cyber incidents including ransomware incidents, therefore it makes no sense to require those entities to report under a separate ransomware reporting regime, as proposed.

- Consideration should be given to introducing **a 'materiality' threshold for reporting ransomware incidents**, such as number of affected devices or personnel involved in responding.
- The threshold for reporting obligations exempts organisations with an annual turnover of $10 million or less (that is, most businesses in Australia) which is reasonable given the compliance challenges smaller organisations would face. However, such businesses may often be third-party providers in the university system, which highlights the imperative for Government measures to assist such organisations in addressing the broader ransomware challenge.
- The SOCI Act includes provisions for the treatment of unincorporated foreign companies to be treated as entities under the Act, albeit with some changes. Consideration should also be given to how organisations domiciled overseas but conducting business in Australia and collecting personal data, should be addressed under ransomware reporting requirements.

It should be noted that universities already have cyber reporting obligations under several initiatives not limited to the SOCI Act, for example under the Guidelines to Counter Foreign Interference in Universities (UFIT Guidelines), as part of membership of the Defence Industry Security Program, privacy obligations, Australian or international research funding requirements, and State Government legislation.

RECOMMENDATION 2

The higher education and research sector experienced significant regulatory impact when it was brought under the purview of the SOCI Act, particularly caused by what is meant by 'critical infrastructure' within the university's activities and the meaning of 'education asset'. To reduce unnecessary organisational impact of the proposed reforms, there should be further guidance or qualification of major elements, such as underpinning criteria regarding what the reforms would aim to protect.

Go8 members note that difficulties in complying with the SOCI Act stem from a lack of clarity e.g. definitions, as well as overlap or conflict with existing obligations, rather than a lack of willingness or capability. Go8 members report that it has been operationally burdensome to identify and manage a list of SOCI-relevant assets in the context of a research-intensive university.

One Go8 university has elected to advise the Australian Signals Directorate (ASD) routinely of any material cyber security incidents to limit the potential for breaching its obligations under the SOCI Act, and to support ASD in their awareness of cyber security threats impacting the university. One of the larger Go8 universities notes that given the complexity of its environment and the breadth of the SOCI Act, multiple teams within the University work together to ensure that the SOCI requirements are well understood and appropriate operational measures embedded, to ensure compliance.

While the Go8 acknowledges the Department's intent for reforms to be informed by stakeholder experience, including definition of key terms, **more context and clarity is needed regarding what is intended by the major elements** to be captured by the reforms.

For example, while '**business-critical data'** is defined in the SOCI Act, largely with respect to its relationship to critical infrastructure assets, universities would find it challenging to determine what is in scope and what is not in scope.

- For universities, 'business-critical data' would include data from all major functions – including research, teaching and learning, and corporate, but will not be all data.
- Nor would 'business-critical data' for the purpose of Measure 5 on 'Data Storage systems and business critical data' be ALL data referred to in the definition in the SOCI Act. An example may be derivative data, that can be computed again, in the case of research supported by a high-performance computer – even though part (b) of the definition in the SOCI Act refers to 'information relating to any research and development in relation to a critical infrastructure asset'.
- Relevant university data would often be personal information, which is regulated under numerous privacy laws, under both State and Federal legislation. The additional requirements under the SOCI Act should be specific and prescriptive to avoid confusion or duplication with similar obligations.

Without a clearer understanding of 'business-critical data', it would clearly be difficult to determine which '**data storage systems that hold business-critical data'** will be impacted by Measure 5. This is further complicated by the expectation in the Consultation Paper that such systems would need to be considered "where vulnerabilities in these systems could have a 'relevant impact' on critical infrastructure". We note that:

- University data storage assets often deliver service to multiple functions within the organisation, which adds to the complication and therefore costs of compliance. Many organisations will have to invest significantly more time and effort into striking a balance between security, usability, and operational realities.
- University systems are not traditionally those on which an attack would cause a major outage of essential services and the disruptions which these reforms seek to avoid or mitigate.
- Universities use third-party data storage providers for some of their needs, which means that they will need to consider how to manage that provision to accommodate additional requirements introduced under these reforms.

The understanding of business-critical data would also affect how '**Material risk'** is determined.

In relation to Measure 7 on Government sharing information in crisis situations, further clarity and contextualisation of '**harms-based approach'** is needed to guide entities in determining what potential harm or risk may result from disclosing information. The Go8 notes that some universities may hold PROTECTED, SECRET and TOP SECRET classified information which accrue specific obligations and restrictions, which in turn would limit the university's ability to share information in the event of an incident.

RECOMMENDATION 3

The Go8 agrees that the proposed obligation on the Australian Signals Directorate and the National Cyber Security Coordinator (Measure 3) to encourage industry to voluntarily provide information to both agencies about a cyber incident needs to be limited use. However, there needs to be further clarity on how this would be implemented, and how the constraints on sharing and use of incident information will be monitored and enforced. A limited use obligation must have a clear 'value-add' benefit for the impacted party as well as for the Government, for example through more formal engagement such as a 'dedicated line' to expert Government advice. Consideration should also be given to introducing protections to minimise reputational risk to the impacted organisation if the engagement with ASD or the NCSC is mishandled or miscommunicated.

The Go8 emphasises that any requirements arising from the limited use obligation would need to align with and not duplicate existing mandatory reporting consistent with Go8's Recommendation 1.

It is important to note that Go8 universities already engage with a range of bodies during significant cyber incidents including ASD and the Australian Cyber Security Centre (ACSC), as well as ASIO and State Government bodies. Our universities have ongoing engagement with the Department of Home Affairs and other Federal Government agencies outside of specific incidents. This is in addition to the reporting that universities are subject to in relation to cyber incidents under the SOCI Act.

RECOMMENDATION 4

The **Go8 strongly emphasises that an all-hazards power of last resort to allow Government to direct an entity to take specific actions to manage the consequences of a national significant incident should ONLY be used where there is no other legislated recourse or powers available, and/or at the request of the impacted entity**. The Go8 does not support intervention if the university is 'unwilling', if this stems from conflicting obligations.

The case for introducing the all-hazards power is insufficiently made in the Consultation paper. More specific criteria are needed to enable affected entities to understand in what situations Government intervention would occur. The Go8 proposes that **consideration be given to redressing identified lack of powers**, as seen in the example regarding Optus and Medibank's inability to share data about affected customers with banks.

Go8 universities have existing incident management processes, and a third party with limited experience and knowledge of a particular university environment may slow the response and divert limited university cyber security resources to engaging with and managing the intervention.

RECOMMENDATION 5

The **case for a Cyber Incident Reporting Board (CIRB) should state more precisely what the merits of such a board should be.** Go8 members undertake careful reviews of major cyber incidents, aided as needed by specialist / dedicated experts. The university sector is also aided by an effective existing ecosystem of threat intelligence sharing across ASD, ASIO, Australasian Higher Education Cybersecurity Service (AHECS), AusCERT, AARNet, and commercial partners and providers.

Consideration should be given to whether the functions proposed should be carried out under the purview of an existing body, such as the new Executive Cyber Council.

Potentially, the CIRB could have a role to play in major cyber incidents affecting numerous sectors or parties, so that lessons and revised approaches informed by the response can be used to improve national or individual strategies. Given the rapidly evolving threat landscape, **timeliness of review and release of lessons learned is critical.**

An alternative may be to encourage Australian organisations to voluntarily share their post incident reports with government (ACSC) under the existing conditions and principles used for mandatory reporting obligations. The Go8 believes that the cyber security industry performs well with respect to identifying root-causes of incidents, making recommendations, and sharing information. Further, specialist incident response and forensic companies are routinely retained and engaged by individual organisations, and they perform a similar function to the proposed CIRB.

If established, there must be clear parameters to identify those cyber incidents that the CIRB should review, to prevent unnecessary and duplicative effort and cost on individual organisations. The CIRB **should include adequate higher education and research sector representation to ensure the sector's unique perspectives and needs are understood.**

OTHER – PROPOSED MEASURE 9

Regarding the proposed Measure 9 on Consolidating telecommunication security requirements – Telecommunications sector security under the SOCI Act, the Go8 agrees that the alignment is reasonable and would further negate having two separate mechanisms with different obligations for different critical infrastructure.

Thank you again for the opportunity to provide this submission. I would be pleased to discuss the contents of this submission in further detail and can be contacted via my Chief Operating Officer, Tracey Wright via e: [redacted].

Yours sincerely,

[redacted]

VICKI THOMSON
CHIEF EXECUTIVE