Department of Premier and Cabinet
Executive Building 15 Murray Street HOBART TAS 7000 Australia
GPO Box 123 HOBART TAS 7001 Australia
Ph: 1300 135 513 Fax: (03) 6233 5685
Web: www.dpac.tas.gov.au

Tasmanian Government

Chair
Parliamentary Joint Committee on Intelligence and Security
E: pjcis@aph.gov.au

Dear Chair

Thank you for the opportunity to respond to the Parliamentary Joint Committee on Intelligence and Security inquiry into the Cyber Security Legislative Package, consisting of:

- Cyber Security Bill 2024;
- Security of Critical Infrastructure and Other Legislation Amendment (Enhanced Response and Prevention) Bill 2024; and
- Intelligence Services and Other Legislation Amendment (Cyber Security) Bill 2024.

Cyber security and the protection of critical infrastructure are essential to protecting our way of life and continued access to essential services.

The Department of Premier and Cabinet is responsible for work across protective security, critical infrastructure and cyber security to enhance Tasmania's security and resilience. We recognise that security is a shared responsibility that requires collaboration across Australian jurisdictions, and we value our ongoing engagement with the Australian Government, other states and territories and our critical infrastructure stakeholders.

The Cyber Security Legislative Package intends to implement initiatives under the 2023-2030 Australian Cyber Security Strategy, and progress and implement reforms to the *Security of Critical Infrastructure Act 2018* (Cth). This submission considers the principles-based policy implications of the measures in the legislative package.

While we have consulted with our colleagues from across the Tasmanian Government, the limited time to respond means that this submission represents the views of my Department. It does not represent the position of the portfolio ministers or the Tasmanian Government.

Cyber Security Bill 2024

In the context of Australia's cyber security landscape evolving quickly, with malicious activities targeting Australia becoming more frequent and sophisticated, my Department supports the creation of a Cyber Security Bill to provide a legislative framework for whole-of-economy cyber security issues.

Security standards for smart devices

My Department supports the need to introduce mandatory cyber security standards for smart devices, noting they are in all Australian homes and businesses where they collect significant volumes of potentially sensitive data about users.

The power, established in the Bill, to make mandatory security standards for smart devices in rules, requiring responsible entities to implement a security standard that is specified by the Minister administering the Act is appropriate and allows flexibility to update standards as required.

The coverage of both manufacturers and suppliers and the requirements around statements of compliance are appropriate. We support the introduction of a baseline set of standards, however we would encourage this set of security standards be regularly reviewed and evolve with cyber threat changes.

Ransomware payment reporting obligations

With ransomware and cyber extortion attacks remaining one of the most destructive types of cybercrime, and noting the limited and inconsistent nature of current reporting and threat intelligence, my Department supports the introduction of ransomware reporting obligations on certain entities.

The reporting timeframe of 72 hours and mandatory reportable information proposed in the Bill are appropriate. The inclusion of a broad range of industries and business in the mandatory reporting will provide for a more accurate picture of the ransomware threat landscape in Australia.

We understand this reporting will support the Australian Government's ability to understand the scope and impacts of the issue, disrupt ransomware and cyber extortion actors, and assist victims of attacks. This understanding is also critical for state and territory governments and we acknowledge the provision in section 29 to allow the sharing of ransomware payment reports with jurisdictions as appropriate.

We support the protections under section 30, restricting the use and disclosure of information for civil or regulatory action, as entities affected by ransomware will then not be discouraged from openly disclosing relevant information due to fear of reprisal. We also support the good faith provision to protect entities from incurring liabilities, such as confidentiality requirements that may exist in contractual arrangements, when complying with these obligations.

Information sharing with government during significant cyber security incidents

Although states and territories have primary responsibility for emergency and consequence management within their jurisdictions, my Department notes the coordination role the National Cyber Security Coordinator serves following significant national-level cyber security incidents in liaising with impacted entities, gathering information from across government and industry, and leading the Australian Government's response to consequences arising from incidents.

Early engagement and the sharing of timely information during emergencies is critical to enable timely incident response and recovery. We acknowledge the need to provide appropriate protections, particularly at the Commonwealth level, to provide assurances to entities during a significant cyber incident. As such, we support the creation of a 'limited use' obligation that restricts how information provided to the Coordinator during a cyber security incident can be on-shared to and used by other Australian Government and state and territory entities. We also support this obligation being applied to the Australian Signals Directorate through the Intelligence Services Amendment (Cyber Security) Bill 2024.

The permitted cyber security purposes outlined in section 10 are appropriate, particularly the provision to allow the sharing of information for the purpose of states and territories responding to, mitigating or resolving a cyber security incident. We understand the intent of the consent mechanism under section 11 is to facilitate the sharing of information to a state or territory government on the basis that the information shared is only to be used and disclosed for limited purposes. My Department welcomes further engagement with the Department of Home Affairs on how this consent mechanism will operate in practice to ensure the efficient sharing of information between the Australian Government and jurisdictions in the event of a cyber incident.

Cyber Incident Review Board

My Department supports the establishment of the Cyber Incident Review Board (CIRB) an independent, advisory body to conduct no-fault, post-incident reviews of significant cyber security incidents in Australia to allow government and industry to learn lessons from these incidents to enhance our collective cyber resilience.

The Bill provides a suitable mechanism for the establishment of a CIRB, and the proposed establishment, functions and powers, and limitations on the use and disclosure of information are appropriate. We support the redaction of sensitive information from review reports before public release and welcome the provisions in section 54 allowing the sharing of protected review reports to state and territories to inform future responses to cyber security incidents.

To keep the Bill principles-based and enable appropriate flexibility, the power for the Minister administering the Act to make rules to ensure the effective operation of the CIRB is appropriate. It is important that states and territories are engaged and consulted when establishing the Terms of Reference for the CIRB.

Security of Critical Infrastructure and Other Legislation Amendment (Enhanced Response and Prevention) Bill 2024

Consequence management powers

My Department notes the policy intent of the consequences management powers, as a last resort, to support a national response to manage the consequences of significant incidents. The inclusion of these powers as part of the expansion of the existing government assistance measures framework under Part 3A of the *Security of Critical Infrastructure Act 2018* (Cth), as proposed, is appropriate and will ensure these powers remain subject to all existing safeguards. This includes comprehensive consultation requirements with the First Minister and relevant Shareholder Minister/s in the impacted jurisdiction/s, and with the entity itself.

We support the proposed approach to not change the intervention request power, ensuring this remains limited to cyber security incidents only. We also welcome the proposed additional safeguard that any action direction requiring an entity to disclose personal information will require agreement from the Minister administering the *Privacy Act 1988* (Cth).

States and territories have primary responsibility for emergency and consequence management within their jurisdictions. The combination of existing emergency management powers, regulation and Tasmanian Government ownership means that the exercise of consequence management powers by the Australian Government would only be required in Tasmania under exceptional circumstances and should not override state-based arrangements. The legislation should clearly state that the proposed consequence management powers cannot be exercised if there are existing powers that would be effective and achieve the same outcome even if the holders of those existing powers select not to exercise those powers to achieve the outcome for strategic or operational reasons.

Protected information provisions

My Department supports the move to provide assurances around the sharing of information for certain purposes, noting unclear protected information use and disclosure provisions in the existing *Security of Critical Infrastructure Act 2018* (Cth) have created a reluctance to share information, reducing collaboration and interoperability.

We support the proposed harms-based approach to the protection of information in the Bill and the associated new definition of protected information to clarify that it is information, which if disclosed, could cause harm to the public, the security of an asset, commercial interests, national security or socioeconomic stability.

We also support the clarification of disclosure provisions to reiterate that entities may share protected information to support the continued operation of an asset or to mitigate risks to that asset. It is our understanding that this provision would allow for the sharing of information across entities and sectors for lessons management and to strengthen sector security.

The swift sharing of information between impacted entities and government during an emergency event is essential. We support the inclusion of emergency management in the disclosure of information provisions, particularly as it relates to critical infrastructure entities in section 43E, to provide assurances around the sharing of information to state and territory governments during an emergency. These provisions should be expanded to include First Ministers, as my Department is responsible for whole-of-government critical infrastructure policy and in some circumstances, the policy function during an emergency.

Enforcing critical infrastructure risk management obligations

My Department notes that this section introduces a compliance review and remedy power for the regulator to issue directions to a responsible entity to address any serious deficiencies that are identified in their critical infrastructure risk management program.

It is appropriate for the Secretary or relevant Commonwealth regulator to be required to give written notice to the affected entity and provide an opportunity for response before deciding to issue a direction to address a serious deficiency in their risk management program. For government-owned entities, the consultation requirements before giving a direction, outlined in section 30AI(6), should also include consulting with the relevant Shareholder Minister/s and First Minister of the relevant jurisdiction.

Further, we expect that this remedy power would not be required in the case of critical infrastructure assets operated by a state or territory government agency. Issues with these facilities can be resolved through discussions between the appropriate ministers.

The full costs to industry of compliance with earlier reforms, such as the Risk Management Program Rules obligation, remain unclear. Tasmania is a relatively small jurisdiction with limited resources to meet additional obligations. Tasmanian Government Businesses play a significant role in providing many essential services, and the costs of complying with regulatory obligations would ultimately be borne by the community (through lower returns to government or higher prices for these services).

The national reforms outlined in this package should be accompanied by an appropriate level of support to industry to minimise the costs of compliance as well as clear guidance material to ensure new obligations are understood.

Thank you again for the opportunity to comment on the Cyber Security Legislative Package.

Your sincerely

Shane Gregory
Associate Secretary

22 October 2024