TechCouncil
of Australia

Cyber Security Legislative Reforms

Tech Council of Australia Submission

March 2023

techcouncil.com.au

Executive Summary

Thank you for the opportunity to respond to the consultation on the *2023-2030: Australian Cyber Security Strategy Legislative Reforms*.

The Tech Council (TCA) is Australia's peak industry body for the tech sector. The tech sector is a pillar of the Australian economy and is equivalent to Australia's seventh largest employing sector, with over 935,000 people now working in tech. TCA represents a diverse cross-section of Australia's tech sector, including start-ups, scale-ups, multinational Australian tech companies as well as global tech companies, many of whom provide cyber security services directly to consumers, other businesses, and government.

This submission is structured in four parts.

1. First, we present a **tech industry perspective on the proposed legislative reforms.** We share the Government's vision that Australia can become a world leader in cyber security by 2030 and believe that modernisation of our regulatory framework is one of the important foundations for enhanced cyber resilience. We are encouraged by the collaborative, co-design approach, and efforts to develop trust with industry to uplift our overall cyber security posture as a nation.
2. Second, we outline **key considerations for Government in progressing the reforms.** This includes focusing the reform agenda on simplification, clarification and incentivising good behaviour; fostering a better culture of cooperation and coordination between government, industry, and the broader community; ensuring coherence and coordination across the domestic regulatory landscape, and interoperability with international standards; and adopting overarching principles for best practice regulation of emerging technologies and the digital economy.
3. Third, we present a **TCA response to Part 1 of the consultation paper on new cyber security legislation**. This includes our support for mandatory IoT standards with some refinements to the model, options to improve the design of mandatory ransomware reporting, recommendations to ensure the limited use obligation delivers on its intended purpose, as well as recommendations for the Cyber Incident Review Board's scope, functions, powers, and governance.
4. Finally, we provide our **TCA response to Part 2 of the consultation paper on the proposed amendments to the Security of Critical Infrastructure Act 2018.** This includes recommendations on data storage systems and business critical data, and key issues that need to be considered regarding the consequence management powers, and CIRMP review and remedy powers. We also support and endorse the work currently underway to adapt telecommunications sector security within SOCI.

A summary table of our TCA recommendations can be found overleaf. We would be pleased to continue this dialogue with the Government and discuss our submission in further detail to help support the final design and adoption of the cyber legislative proposals.

Summary of TCA recommendations

Recommendations for the Cyber Security Legislative Proposals	
Secure-by-design standards for IoT Devices	
Recommendation 1.	Adopt mandatory secure-by-design standards for IoT devices that are principles-based and aligned and interoperable with international approaches, by leveraging the ETSI standards or similar.
Recommendation 2.	Provide further guidance on the legal obligations for breaches of the standard across the supply chain, and the reasonable steps Australian entities should take to ensure their obligations are met in relation to other parties in the supply chain (e.g. use of contractual warranties confirming that an IoT product meets the standard).
Recommendation 3.	Adopt a broad definition of 'connected devices' that are captured by the standards and provide exemptions for devices that are already regulated, or higher risk devices that are not "consumer-grade" and may require a different/higher standard.
Ransomware Reporting	
Recommendation 5.	If adopting mandatory ransomware reporting, ensure: a) reporting obligations are aligned to a notification timeframe of 72 hours, consistent with requirements under SOCI and NDB; and, b) ransomware reporting obligations are phased in only after the limited use obligation is in place, and consider including 'no fault, no liability' protections in the legislation.
Recommendation 5.	a) To enhance overall cyber security posture, we think it is important to include small businesses in the mandatory reporting scheme while considering ways to reduce the regulatory burden (e.g. by applying a more simplified and streamlined reporting requirement and a more lenient compliance and enforcement regime). However, if the Government chooses to adopt an exemption then we recommend considering aligning this to a $3 million revenue threshold, consistent with the AML / CTF Act and the Privacy Act.
Recommendation 6.	Continue work to develop a streamlined Single Reporting Portal for cyber incident reporting and integrate ransomware reporting within this process.
Limited Use Obligation	
Recommendation 7.	Limit and reduce the scope of the purposes within limited use, in particular to clarify the purposes of 'informing ministers and government officials' and 'agencies for law enforcement'.

Recommendation 8.	Make explicit in legislation, the accompanying regulations, and/or rules the purposes for which information cannot be used and who it cannot be shared with. This should include specifying: a) That information provided by a disclosing entity will not be used in a way that has legal or reputational repercussions (or words to that effect); b) That information provided be a disclosing entity and shared by the ASD to another government agency will be treated confidentially, with NDAs or other appropriate mechanisms used to ensure that that information will not be further shared or used for punitive actions; and, a) Guidelines or rules to ensure that regulators and law enforcement agencies do not misuse information disclosed to inappropriately bypass information gathering powers within their authority.
Recommendation 9.	Government to uplift and safeguard its own information security practices and methods to ensure information transfer occurs in secure transfer environments and channels.
Cyber Incident Review Board	
Recommendation 10.	Consider integrating the cyber incident review functions and powers within the NCSC to enable a single and streamlined point of responsibility for cyber incident coordination and review, supported by an expert review board, and evolve the NCSC to be established as a statutory authority.
Recommendation 11.	Regardless of the model chosen, affirm that the review mechanism should: a) Have a principal mandate to gather lessons learnt for continuous cyber improvement; b) Adopt a broader remit beyond major one-off incidents to gain a holistic picture of cyber health and cyber threats. c) Safeguard information disclosed to the board from regulatory intervention or law enforcement mechanisms; d) Adopt a no blame approach and culture; and, a) Minimise complexity in reporting and disclosure obligations for entities.
Recommendations for the *Security of Critical Infrastructure Act 2018*	
Data storage systems and business critical data	
Recommendation 12.	Reconsider the adoption and introduction of this proposal in its current form and instead, integrate 'data storage systems and business critical data' as a factor in RMF programs, rather than being established as a separate 'asset'.

Recommendation 13.	Continue bolstering other regulatory and legislative mechanisms, such as privacy and digital ID, to protect customer data and privacy.
Consequence management powers	
Recommendation 14.	Undertake a review of existing consequence management arrangements, leveraging the expertise of the Australian Crisis Coordination Centre (CISC) and the newly established National Office for Cyber Security (NOCS), prior to adopting this proposal.
Recommendation 15.	Prior to adopting this proposal, further clarify: a) How this amendment will ensure steps are taken to appropriately understand an entity's technical and operational context without adding further complexity, b) Interactions with directors duties and legal obligations, c) Scope of responsibility and liabilities for other entities not directly affected by cyber incidents; and, a) Appropriate review and appeal mechanisms that would be provided to affected entities.
CIRMP review and remedy powers	
Recommendation 16.	Before adopting this proposal, further clarify the: a) Risk profiles of entities for the CIRMP review and remedy proposals; b) Definition of 'seriously deficient'; c) Factors and considerations for assessment; a) Apportionment of legal liability where there is an intervening direction by Government resulting in a cyber incident.
Recommendation 17.	Reconsider the efficacy of activating penalties within the current voluntary scheme, which may hinder uptake and adoption.
Telecommunications sector security under the SOCI Act	
No recommendations – proceed and endorse the work of the Australian Telco Security Reference Group.	

1. A tech industry perspective on the proposed legislative reforms

Cyber security is one of the highest priorities for the Tech Council and our members. The recent high profile data breaches and cyber-attacks Australia has experienced, combined with the rise of emboldened state-based actors, warrants a comprehensive and collaborative response that unites government and industry to improve our national cybersecurity readiness and resilience.

The Tech Council shares the Government's vision that we can be a world leader in cyber security by 2030. We have the right foundations for a world-class cyber security environment, and we can continue to work to improve coordination, as well as increase the effectiveness of our prevention and post-incident response mechanisms.

Improving Australia's national cyber security posture isn't just a matter of national security, it is also central to the growth of our digital economy, and more importantly, a fundamental underpinning to our economic strength and social stability.

Our positions are informed by our expert cyber group which was initially convened after the large-scale cyber incidents in late 2022. Since then, we been deeply engaged in the Government's work and progress on cyber security. We have previously provided input to help inform the 2023-2030 Cyber Security Strategy and have been engaged on a number of other issues on cyber security. This includes ACSC's secure-by-design initiatives and Home Affairs and ASD's consultation on an interim limited use obligation.

We welcome the progress that has been made to date on the Strategy and the Government's intent for the proposed legislative reforms and amendments to address gaps in the existing regulatory framework.

We are encouraged by the collaborative and co-design approach that Government has adopted for the consultation process, as well as other broader cyber security initiatives such as the work underway in the Executive Cyber Council, to ensure that reforms are practical, internationally coherent, while appropriately minimising regulatory burden for businesses in Australia.

We also welcome Government's efforts to develop and build trust with industry on cyber security, including on issues of intelligence and threat sharing, which underscores the foundational understanding that we all have shared responsibilities to help lift our cyber preparedness and resilience as a nation.

We would also like to highlight that there are a range of technologies and tools developed by industry that can assist and support our collective efforts in enabling us to achieve the outcomes of the proposed legislative reforms. This includes the adoption of emerging technologies such as AI and quantum computing that have the potential to bolster cyber detection and response.

Becoming a world leader in cyber security – underpinned by a thriving tech workforce and ecosystem – can provide Australia with a competitive economic advantage, underpinning our shared effort with the Australian Government to reach 1.2 million tech jobs and increase the tech sector's economic contribution to $250b annually by 2030.

2. Key considerations for Government in developing a legislative response for cyber security

We encourage the Government to take account of the following considerations when progressing the legislative reforms.

2.1 A reform agenda focused on simplification, clarification, and incentivising good behaviour

At present, numerous agencies hold varying degrees of responsibility for cyber regulation, compliance, and response. It is already a complex and crowded space with an array of entities with some level of responsibility for cyber security.[1] Efforts to streamline governance and administration, as well as minimise duplication and redundancy, are vital aspects in creating an effective and responsive cyber security legislative framework.

The Government should endeavour to ensure that any terms and definitions proposed are clearly defined and unambiguous to help foster compliance. Appropriate supporting guidance will also support the effective interpretation and application of any legislation that may be introduced. Moreover, clear and simplified obligations will also help organisations understand their responsibilities and take the appropriate actions to better enable compliance.

Finally, a move beyond rigid rule or penalty-based approaches will also help incentivise the positive behavioural change we wish to see. As we seek to inspire genuine change, a move towards outcomes-based, flexible, adaptive, and incentive-driven strategy becomes a key enabler. An approach that incentivises positive behaviours also encourages industry to invest in cyber security measures that will enable us to progress towards a culture of shared responsibility across the whole of our Australian economy and society.

2.2 Fostering a better culture of cooperation and coordination between government, as well as with industry and the broader community

In light of the escalating global threat environment, enhancing cooperation and coordination between government, industry, and the broader community is crucial in bolstering our overall cyber security resilience and posture. This collaboration and coordination needs to be across the full suite of cyber activities from threat intelligence sharing and threat blocking, to incident consequence management and post-incident response and review.

We support and continue to encourage the Government's efforts in improving trust and cooperation. This includes actions to streamline processes for preventing, disclosing, and responding to cyber incidents, as well as bolstering collaboration mechanisms to address evolving threats effectively.

Greater cooperation on activities that can prevent or minimise cyber incidents, such as sharing of threat intelligence, is seen as particularly valuable by industry to improving cyber

[1] At the federal level this includes but is not limited to: Home Affairs, the Australian Signals Directorate, Australian Cyber Security Centre, Department of Defence, Attorney-Generals Department, Office of the Australian Information Commissioner, Australian Federal Police, Australian Communications and Media Authority, Australian Securities and Investments Commission, Australian Prudential Regulatory Authority, and the eSafety Commissioner, and more. This list also doesn't take into account the interests of other federal departments in cyber security policy, and the many state and territory agencies that have an operational role.

security and needs to occur on a two-way basis. We have a joint role to play in prioritising the establishment of trust-based relationships, facilitating open communication, as well as mutual and reciprocal support.

2.3 Coherence and coordination across the domestic regulatory landscape, as well as through international standards and harmonisation

We support the Government's ambitious regulatory reform agenda to modernise and evolve the legislative landscape for a digital age. In adopting these legislative changes, it is important that Government appropriately considers existing regulation to ensure alignment for a coherent domestic regulatory landscape. These proposals should also be closely aligned to other review and reform processes underway including with the Privacy Act Review, Safe and Responsible AI, national Digital Identity framework, Online Safety, and the recent work on mandatory reporting for scams.

Given the global context in which Australia operates, we are encouraged by and support the Government in adopting an approach that prioritises international interoperability and harmonisation. Leveraging global standards and best practice for an Australian context not only enhances the nation's cyber resilience and facilitates smoother collaboration and information sharing with our international allies and partners, it also minimises regulatory costs on businesses.

2.4 Best practice regulation of emerging technologies and the digital economy

We encourage the Government to consider a set of overarching best practice principles and to keep these in mind while proceeding with the reforms:

- *Informed and coordinated* – underpinned by rigorous analysis and industry engagement, with thoughtful consideration of the interrelationships with regulations
- *Proportionate* – taking a risk-based and outcome-based approach to address clearly defined problems and gaps
- *Timely* – responsive to the changing threat environment and be cautious in moving too far ahead of overseas jurisdictions in a way that could disadvantage Australian industry
- *Consistent and interoperable* – including with global and domestic regulation to improve the ease of doing business and maintain Australia's investment attractiveness
- *Supports innovation and growth* – by avoiding prescriptive technical requirements that may quickly become outdated or inhibit innovation, and by enabling new technologies that can help improve the risk environment to provide Australia with a competitive advantage in the digital age.

3. TCA Response to new cyber security legislation proposals

3.1 Secure-by-design standards for IoT devices

We recognise that there is considerable scope to improve secure tech development standards and guidance, including with respect to IoT devices. Security-by-design and default remains a relatively nascent area in Australia and internationally, but IoT policy and regulation is an area that is relatively more mature in other jurisdictions. We therefore support the Government adopting an approach that prioritises international interoperability and harmonisation, by adopting the ETSI EN 303 644 standard as the basis for reform, given this standard underpins other regulatory frameworks overseas.

We have no concerns with enshrining the first three principles of the ETSI standards in legislation (i.e. removal of universal passwords, receiving reports of cyber vulnerabilities, providing information on minimum security update periods for smart device software).

With regard to responsible entities named in the discussion paper – manufacturers, subcontractors, software developers, importers, distributors – we believe that these are the appropriate entities for this to apply. A consistent standard across the supply chain will ensure all parties adhere to unified requirements.

However, we also encourage the Government to provide further guidance on the practical implementation of this proposal, particularly given Australia's significant reliance on imported manufactured devices. The shared roles and responsibilities of different actors in the supply chain differ depending on the type of component provided. The effectiveness of this measure is anchored on the ability to enforce compliance among overseas entities, with supply chain management involving multiple parties across different jurisdictions with varying regulatory requirements and enforcement mechanisms. Clarity is needed on how entities will coordinate with international manufacturers, distributors, and other stakeholders to uphold cyber security standards throughout the importation process.

We also seek further clarity on the consequences and legal obligations for breach for liability in the supply chain, which is uncertain. It would be helpful to provide examples of reasonable steps that an entity should take in ensuring adherence to the standard. For example, one way of doing this would be clarifying that contractual warranties confirming that an IoT product meets the standard are sufficient. There are also emerging concepts and mechanisms to enhance visibility and traceability in manufacturing supply chains. For example, the use of "digital threads" being applied to IoT devices to provide a digital representation of a product's lifecycle, giving a more complete and transparent view of manufacturing across the supply chain.

With regard to the devices in scope for the mandatory standard, we support a broad definition of 'connected devices' or similar (e.g. the UK, which uses the term 'relevant connectable products'). We also agree exemptions should be considered for connected products that are already regulated through other mechanisms, or higher-risk devices that are not "consumer-grade" and may require a different/higher standard. This ensures that the approach to mandatory IoT devices is risk-based and minimises regulatory burden. Examples of exclusions include devices such as smart meters, charging stations for e-vehicles, distributed energy devices and medical devices, which should be out of scope.

Secure-by-design standards for IoT Devices

Recommendation 1.	Adopt mandatory secure-by-design standards for IoT devices that are principles-based and aligned and interoperable with international approaches, by leveraging the ETSI standards or similar.
Recommendation 2.	Provide further guidance on the legal obligations for breaches of the standard across the supply chain, and the reasonable steps Australian entities should take to ensure their obligations are met in relation to other parties in the supply chain (e.g. use of contractual warranties confirming that an IoT product meets the standard).
Recommendation 3.	Adopt a broad definition of 'connected devices' that are captured by the standards and provide exemptions for devices that are already regulated, or higher risk devices that are not "consumer-grade" and may require a different/higher standard.

3.2 Ransomware reporting

We understand the primary purpose of this reporting proposal is to gather information to build a more comprehensive and complete picture of the extent and scale of ransomware occurring in Australia, to help adapt our policy and operational settings.

To Ienable a genuine 'no-fault, no-liability scheme', we recommend that the reporting requirement be phased in *only after* the limited use obligation is in place, especially if the intention of the reporting obligation is to improve information sharing and understanding of cyber incidents in Australia. Alternatively, or as a complementary measure, the Government should consider adopting the principles of 'no fault, no liabiity' in the legislation for the reporting regime, and make explicit in the legislation that information provided through ransomware reporting will not be used for subsequent regulatory, legislative or punitive actions.

If adopted, we also suggest the following recommendations to:

- Align with reporting obligations under other regimes including the Notifiable Data Breaches (NDB) scheme under the Privacy Act and requirements under SOCI, to clarify that the time for notification will be 72 hours from the time of being aware of an incident. This will help support consistency and alignment in reporting timeframes across the whole legislative framework.

- Ensure reporting is more integrated and streamlined across the variety of existing reporting regimes to reduce duplicative efforts by businesses in providing similar sets of information for similar purposes. This could be done through the ASDs/ACSC's new Single Reporting Portal for cyber incidents.

- Consider broadening the definition of 'cyber extortion' beyond data encryption/decryption referred to in the discussion paper as there are also examples of attacks like DDos attacks, doxing, vulnerability extortion, security threats etc. that are relevant.

Regarding small businesses, we caution against exempting small businesses because an exclusion may have potential unintended consequences by creating a perverse incentive for cyber attackers to target small businesses who fall under the threshold. If the purpose of the reporting regime is to build a more comprehensive picture of the ransomware threat, it also doesn't make sense to include the majority of businesses operating in Australia.

However, if the Government choses to adopt an exemption, we recommend it consider aligning the reporting threshold for organisations to the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (AML/CTF) and the Privacy Act, with a revenue threshold of $3 million. Additionally, we recommend the Government design a separate, simplified and streamlined reporting process to ensure that compliance and enforcement is easy for small business operators.

Ransomware Reporting	
Recommendation 5.	If adopting mandatory ransomware reporting, ensure: c) reporting obligations are aligned to a notification timeframe of 72 hours, consistent with requirements under SOCI and NDB; and, d) ransomware reporting obligations are phased in only after the limited use obligation is in place, and consider including 'no fault, no liability' protections in the legislation.
Recommendation 5.	To enhance overall cyber security posture, we think it is important to include small businesses in the mandatory reporting scheme while considering ways to reduce the regulatory burden (e.g. by applying a more simplified and streamlined reporting requirement and a more lenient compliance and enforcement regime). However, if the Government chooses to adopt an exemption then we recommend considering aligning this to a $3 million revenue threshold, consistent with the AML / CTF Act and the Privacy Act.
Recommendation 6.	Continue work to develop a streamlined Single Reporting Portal for cyber incident reporting and integrate ransomware reporting within this process.

3.3 Limited use obligation

We support the Government's intent to establish a limited-use obligation for information sharing as well as the Government's efforts to work with industry by helping boost information-sharing and strengthening relationships. We acknowledge that trust needs to be developed over time, requiring effort, transparency, genuine communication and collaboration.

However, we also note that there is a legitimate and serious concern from businesses regarding the potential legal risk, action, and liability for organisations when disclosing information to the ASD. Once information is disclosed, dissemination of this information to other organisations, departments, agencies, regulators (who may also be clients of the disclosing entity), media, or other public domains also raises the risk of misinterpretation or reputational damage due to inaccurate or incomplete contextual information.

In particular, the purposes of 'informing ministers and government officials' and 'sharing information with other agencies for law enforcement' raises a number of further concerns that need to be addressed, or the proposal risks not achieving its intended objective of improving information sharing and government/industry collaboration. The sharing of information for these purposes may trigger actions by other parts of Commonwealth machinery resulting in the potential of regulatory or punitive actions, despite suggestions that this would not be allowed. Law enforcement or regulatory agencies may use the sharing of information for genuine cyber security enhancement to bypass proper judicial process to access that information for use in subsequent prosecutions or regulatory actions – appropriate safeguards need to be in place for companies to ensure information is not shared and used in this way.

As such, the Government should not only clarify the prescribed cyber security purposes for which information can be used, it should also explicitly clarify in legislation or accompanying regulations the purposes for which information cannot be used and who it cannot be shared with. This includes explicit safeguards that prevent shared information being used in a way that has legal or reputational repercussions, and appropriate requirements for confidentiality of shared information to provide assurance and create a safe environment for information sharing.

While we support the work currently underway to adopt guidelines that help inform interactions with regulators, to ensure that they adhere to their own investigatory and discovery powers and functions to safeguards against potential misuse of authority, we suggest that these efforts are bolstered by enshrining this within legislation or the accompanying regulations.

There should also be requirements for transparency from ASD with the disclosing entity to inform them about the next steps following sharing of information (i.e. what will happen, who this information will be shared with, who will be briefed etc.).

We also recommend that Government uplift and safeguard its own information security practices and methods. This is to ensure that information transmitted across Government entities occurs is a secure transfer environment and uses secure communication channels.

Limited Use Obligation	
Recommendation 7.	Limit and reduce the scope of the purposes within limited use, in particular to clarify the purposes of 'informing ministers and government officials' and 'agencies for law enforcement'.
Recommendation 8.	Make explicit in legislation, the accompanying regulations, and/or rules the purposes for which information cannot be used and who it cannot be shared with. This should include specifying: c) That information provided by a disclosing entity will not be used in a way that has legal or reputational repercussions (or words to that effect); d) That information provided be a disclosing entity and shared by the ASD to another government agency will be treated confidentially, with NDAs or other appropriate mechanisms used to ensure that that information will not be further shared or used for punitive actions; and, e) Guidelines or rules to ensure that regulators and law enforcement agencies do not misuse information disclosed to inappropriately bypass information gathering powers within their authority.
Recommendation 9.	Government to uplift and safeguard its own information security practices and methods to ensure information transfer occurs in secure transfer environments and channels.

3.4 Cyber Incident Review Board (CIRB)

We support the concept of an incident review mechanism to ensure all parties can learn the lessons from cyber security incidents and promote best practice across the economy. This has been one of our previous recommendations and the TCA are pleased to see it reflected in the current legislative proposals.

However, this current proposal seeks to establish the Cyber Incident Review Board (CIRB) as a separate, standalone entity from the NCSC and other government entities. This creates risks of additional complexity in the overall regulatory and governance framework for cyber security, additional reporting burden and coordination challenges. We caution that this model may counter the broader efforts and objectives in the Cyber Security Strategy to streamline reporting processes, duplicative efforts, and bureaucratic processes.

We have previously recommended that the NCSC to be established on a statutory basis in order to effectively coordinate the response to major cyber incidents as well as undertake post-incident reviews. In addition to having a single point of contact for cyber incidents, this arrangement would have the additional benefit of being able to appropriately sequence and prioritise requests for information and reporting from various agencies, departments, and others.

While we acknowledge there is a potential tension and trade-offs with NCSC's coordination function working across whole-of-government vis-a-vis a potential review and assessment function for incidents, we suggest that appropriate quarantine processes, firewalls, and confidentiality protocols could be set up to address this.

As such, we maintain our previous position and recommend evolving the NCSC as an independent statutory authority which would also enable the NCSC to conduct genuinely independent reviews. The review function of the NCSC could then be supported by an independent expert advisory group, in the form of a "Board" or something similar for cyber incident review, with experts drawn from industry and government.

If Government chooses to continue with the current model, we emphasise that it will be crucial for the CIRB to possess a clear mandate, delineated authority, and sufficient resources to execute its responsibilities independently, free from undue influence or interference, while encouraging coordination with other arms of government. Government may wish to consider appointing the NCSC to the CIRB in some capacity to ensure that the CIRB is appropriately aligned to other cyber incident and reporting processes.

We also recommend considering the following points in standing up the review mechanism, regardless of the model chosen:

- The principal mandate should be gathering lessons learnt for continuous improvement and mechanisms should be put in place to safeguard information disclosed to the Board from being used for regulatory interventions or law enforcement measures.

- It should be closer to the transport review board / aviation safety model in adopting a no-blame approach and culture, while balancing this with openness and transparency to help deliver the insights and intelligence that the government wishes to achieve.

- It should minimise reporting and disclosure obligations for entities who are undertaking or have experienced a cyber incident. Additional reporting and disclosure obligations should not further disrupt operational continuity and divert valuable resources away from critical incident response and/or remediation activities. The functions and powers of the CIRB should not add to that complexity.

- It should adopt a broader remit for cyber incident review and reporting beyond major one-off incidents (e.g. the capacity to consider a series of incidents across multiple organisations) to gain a more holistic picture of cyber health in the economy and identify where action is most needed. This ensures that the lessons learnt from incident reviews can work to effectively address underlying systemic vulnerabilities and threats.

Cyber Incident Review Board	
Recommendation 10.	Consider integrating the cyber incident review functions and powers within the NCSC to enable a single and streamlined point of responsibility for cyber incident coordination and review, supported by an expert review board, and evolve the NCSC to be established as a statutory authority.
Recommendation 11.	Regardless of the model chosen, affirm that the review mechanism should: e) Have a principal mandate to gather lessons learnt for continuous cyber improvement; f) Adopt a broader remit beyond major one-off incidents to gain a holistic picture of cyber health and cyber threats. g) Safeguard information disclosed to the board from regulatory intervention or law enforcement mechanisms; h) Adopt a no blame approach and culture; and, i) Minimise complexity in reporting and disclosure obligations for entities.

4. TCA response to amendments to the *Security of Critical Infrastructure Act 2018*

4.1 Data storage systems and business critical data

The Tech Council appreciates the Government narrowing the focus of this proposal following feedback on the Cyber Security Strategy consultation paper last year. The proposed focus on regulating critical infrastructure data storage systems holding "business critical data" is much more proportionate and appropriately risk-based than the proposal to regulate "customer data and systems."

We maintain that the SOCI Act is intended to apply a higher regulatory standard to a targeted list of facilities and assets that are critical to the functioning and prosperity of Australia's social and economic stability, defence, and national security.

However, there are still some important complexities and challenges that need to be considered in the design of this proposal:

- The term 'business critical data' is subject to varied interpretation which applies across different industries, sectors, organisations, and functions. This raises a significant uncertainty and warrants further consideration and clarification if adopted.
- The practical uptake of this proposal may present difficulties (especially with regard to the obligations, responsibilities and liabilities) where business critical data is hosted on third party servers. SOCI entities may be limited in taking the appropriate steps to ensure the security of those data storage systems. We encourage Government to

provide guidance on how to address this. For example, considering a mechanism for certification or assurance if an entity is using a provider that is subject to the SOCI Act.

- As the discussion paper has also acknowledged, there are also overlaps with the current proposals in the reforms to the Privacy Act, which is seeking to introduce significantly increased penalties for serious breaches of the Privacy Act. There are also a number of overlapping, broader data retention schemes and obligations that SOCI entities must comply with that heightens the regulatory burden for businesses.

To achieve the same outcomes we understand the Government is seeking, we recommend adopting the following measures:

- Incorporate 'data storage systems and business critical data' as factors within the existing Risk Management Framework (RMF) programs, rather than treating them as separate 'assets'.
- Proceed with the proposals in the Privacy Act reforms, in particular enhancing guidance on "reasonable steps" for 'technical and organisational measures' to secure personal information in APP 11 to include cyber security measures, as a means of improving security of data storage systems.
- Continue prioritising the rollout of Digital ID legislation and adoption of Digital ID solutions to better protect customer data and privacy.

Data storage systems and business critical data	
Recommendation 12.	Reconsider the adoption and introduction of this proposal in its current form and instead, integrate 'data storage systems and business critical data' as a factor in RMF programs, rather than being established as a separate 'asset'.
Recommendation 13.	Continue bolstering other regulatory and legislative mechanisms, such as privacy and digital ID, to protect customer data and privacy.

4.2 Consequence management powers

While the rationale in the consultation paper for introducing this amendment refers to the need to manage secondary consequences, we have significant reservations on the proposed expanded powers and the efficacy of these measures.

The existing Part 3A of the SOCI Act already encompasses step-in powers. Notably, these step-in powers have not been fully exhausted since the Act has come into force and a more comprehensive evidence base to justify the policy rationale would be beneficial. Additional examples demonstrating the shortcomings or ineffectiveness of current measures would bolster the case for introducing the proposed amendment. In its current form, we suggest that the proposal should be limited to how Government manages its own systems and processes.

As such, we recommend that the Government undertake a review of existing crisis response arrangements and make improvements to these processes before adopting this amendment. For example, the Government should leverage established entities such as the Australian Crisis Coordination Centre and the recently established Cyber Security Response Coordination Unit within the NOCS, to identify and implement more effective strategies for working with the affected entity to support consequence and incident management.

This approach would also signal to industry and the broader community the Government's commitment to fostering a better culture of cooperation and coordination, while helping to build trust and facilitate information sharing.

Moreover, the proposed expansion of ministerial involvement in business cyber response also raises a number of concerns:

- Directives may not align with the contextual, operational, and technical nuances of the affected entity. Organisations may be hesitant to fully engage with government entities if they perceive them as intrusive or lacking in the necessary contextual, technical, or operational understanding to provide meaningful support. This has the potential to create an additional layer of complexity in incident response.
- The perception of government overextension into business cyber response has the potential to erode trust and cooperation between government agencies and the private sector, which would in turn undermine collaborative efforts to improve the effectiveness of public-private collaboration in enhancing cyber resilience.
- There are also legitimate issues regarding director's duties and potential conflicts. Directors may find themselves in a precarious position with regard to their existing statutory duty and legal obligations as directors working for the best interests of their organisations.
- There is also uncertainty for this amendment to create additional obligations and potential liability for other entities ('secondary entities') where it's not appropriate in that they aren't directly impacted or responsible for the cyber incident.
- The absence of a clear review mechanism for entities to appeal or challenge a direction is problematic. It is unclear what the appropriate avenue or forum would be for a process of appeal whether through judicial review, or administrative tribunal.

Consequence management powers	
Recommendation 14.	Undertake a review of existing consequence management arrangements, leveraging the expertise of the Australian Crisis Coordination Centre (CISC) and the newly established National Office for Cyber Security (NOCS), prior to adopting this proposal.
Recommendation 15.	Prior to adopting this proposal, further clarify: d) How this amendment will ensure steps are taken to appropriately understand an entity's technical and operational context without adding further complexity, e) Interactions with directors duties and legal obligations, f) Scope of responsibility and liabilities for other entities not directly affected by cyber incidents; and, g) Appropriate review and appeal mechanisms that would be provided to affected entities.

4.3 CIRMP review and remedy powers

This proposal seeks to establish a formal directions power to address 'seriously deficient elements' of CIRMPs. We seek further clarification on a number of aspects of this proposal.

- We strongly encourage Government to clarify risk profiles of entities for this proposal. It is important to acknowledge that risk-management plans are not a one-size-fits-all endeavour. Each SOCI entity operates within a unique context, with distinct threats, vulnerabilities, and potential impacts and harms. As such, risk management plans are heavily tailored to the organisation, its customers, the industry sector, business and operating models, as well as technological infrastructure. Further guidance or examples would be beneficial.

- The term 'seriously deficient' and the processes for this determination with respect to authorising the directions power would benefit from further clarification. This includes further refinement of the factors and considerations that the Secretary of Home Affairs or relevant Commonwealth Regulator may use to make this assessment. Further guidance would be beneficial.

- In the event that a directions power is authorised and complied with, there is also uncertainty with regard to the apportionment of responsibility and legal liability for a scenario where a cyber incident consequently results from a Government direction. While the intent may be to enhance and remedy a 'deficient' CIRMP, these actions could inadvertently contribute to or exacerbate cyber security risks.

- While Government is looking to move towards a greater compliance and enforcement strategy for this proposal, we note the counter-incentive created between the current voluntary nature of reporting on the CIRMP obligation and the mechanism in the proposal to now enforce penalties (250 penalty units) under this voluntary scheme which runs counter to the existing educative and collaborative approach that CISC has been undertaking.

CIRMP review and remedy powers	
Recommendation 17.	Before adopting this proposal, further clarify the: d) Risk profiles of entities for the CIRMP review and remedy proposals; e) Definition of 'seriously deficient'; f) Factors and considerations for assessment; g) Apportionment of legal liability where there is an intervening direction by Government resulting in a cyber incident.
Recommendation 18.	Reconsider the efficacy of activating penalties within the current voluntary scheme, which may hinder uptake and adoption.

4.4 Telecommunications sector security under the SOCI Act

We endorse the work of Australian Telco Security Reference Group being led by the Department of Home Affairs and the Department of Infrastructure, Transport, Reigonal Development, Communications and the Arts in working with telecommunications companies to align the TSSR security obligations and the RMFs in the SOCI Act.

Telecommunications sector security under the SOCI Act
No recommendations – proceed and endorse the work of the Australian Telco Security Reference Group.