



Protecting Critical Infrastructure and Systems of National Significance

Victorian Government Submission

Table of Contents

Executive Summary	2
1. Introduction	3
2. The need for reform	3
3. Defining the Scope and Application for Reform	4
3.1 Sectors	4
3.2 Entity Level.....	4
3.3 Defining Criticality	5
4. Delivering Inclusive and Representative Governance Arrangements.....	5
4.1 State Government	6
4.2 Industry.....	6
5. Developing Targeted Obligations and Supports.....	7
5.1 Positive Security Obligation.....	7
5.2 Enhanced Cyber Security Obligation.....	8
Information and Intelligence Sharing.....	8
Data Security.....	8
5.3 Cyber Assistance for Entities	9
6. Establishing a Best-Practice Regulatory Model.....	9
6.1 Regulators	9
6.2 Regulatory Burden	9
6.3 Standards	10
6.4 Compliance and Enforcement	10
6.5 Cost Burden	11
7. Establishing Appropriate and Proportionate Commonwealth Powers.....	11
7.1 Declaration of an emergency.....	11
7.2 Ministerial Directions Power	12
7.3 Transparency, Oversight and Safeguards.....	13
8. Concluding Remarks.....	13

Executive Summary

The Victorian Government supports the need to strengthen the security and resilience of national critical infrastructure and systems across all hazards. We recognise the ongoing imperative to deliver capability uplift across critical infrastructure entities and their supply chains to protect the health, safety and prosperity of all Victorians.

That is why following the devastation of the 2009 Victorian bushfires and 2010/11 Floods, Victoria created a comprehensive regime for improving critical infrastructure resilience. Victoria's critical infrastructure resilience arrangements include legislation supporting a risk-based and all hazards approach, partnership between government and industry to build resilience, and a transparent and consistent method for assessing the 'criticality' of infrastructure. These arrangements are supported by a five-year Cyber Security Strategy which outlines the steps we're taking to improve cyber resilience, governance and approach both within government and with Victoria's major infrastructure and service providers. As a State Government with mature critical infrastructure arrangements, we have a comprehensive and end-to-end role to play within the critical infrastructure space.

Victoria therefore welcomes further reforms at a national level to enhance partnerships with industry operators to strengthen all hazards risk management and drive cyber capability uplift. However, significant additional information and consultation is required at all levels of government and with industry to be able to assess whether the proposed arrangements will be fit for purpose and to identify and minimise duplication.

The Victorian Government therefore urges the Australian Government to provide greater clarity on its proposal including additional information that demonstrates the evidence base for the proposed approach, provides clear definition of sectors, outlines the underlying constitutional powers and includes a regulatory impact assessment.

Furthermore, the consultation paper does not outline a clear role for State and Territory Governments. State and Territory Governments operate across critical infrastructure sectors, have responsibilities for managing emergencies within sectors and increasingly are a first line of defence for national security. For these arrangements to be viable, an end-to-end role for State Governments is critical.

There are five critical areas that will need to be worked through to establish a successful national critical infrastructure regime. These are discussed in detail in our submission:

- Adopting a best-practice risk-based all hazards approach across sectors, with a clearly defined scope informed by evidence
- Inclusive and representative governance with an end-to-end role for State Governments
- Establishing a best-practice regulatory model that balances security obligations with the need for investment, sector viability and affordable service delivery
- Developing targeted obligations and supports including timely two-way information and intelligence sharing
- Establishing appropriate and proportionate Commonwealth powers with independent oversight.

Victoria would welcome the opportunity for further engagement to resolve these complex issues and implementation challenges prior to the passage of any legislation.

1. Introduction

The Victorian Government welcomes the opportunity to make a submission on the Australian Government's Consultation Paper *Protecting Critical Infrastructure and Systems of National Significance* released by the Department of Home Affairs in August 2020.

The Victorian Government supports the need to strengthen the security and resilience of national critical infrastructure and systems across all hazards. However, further detail is needed to be able to properly consider and support the proposed reforms. Critical infrastructure reform must be guided by evidence-based outcomes and shared principles, and leverage existing arrangements such as Victoria's own critical infrastructure arrangements. It must balance the need for security and resilience with the need for ongoing investment and the affordability of services for all Australians.

For Australia to successfully deliver capability uplift across critical infrastructure, arrangements will need to clearly articulate an end-to-end role for State and Territory Governments (State Governments). Not only are State Governments investors, owners, operators and regulators of critical infrastructure but we also lead emergency response. State Governments are increasingly a first line of defence for national security. Moving forward, a partnership approach between the Commonwealth and States should be embedded in arrangements to deliver inclusive governance, two-way information flows and minimise regulatory burden.

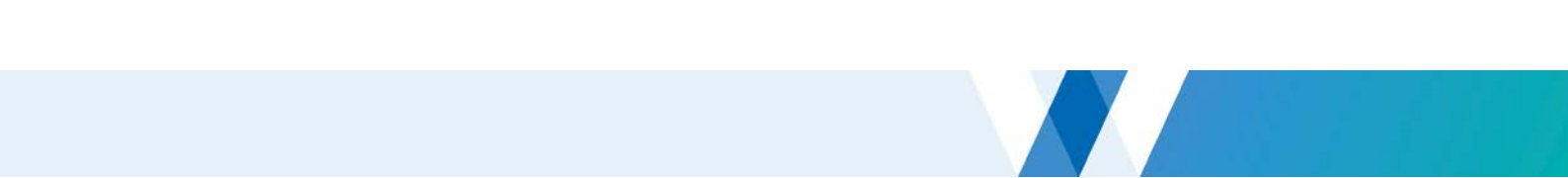
2. The need for reform

Victoria supports the ongoing need to uplift national critical infrastructure security and resilience to respond to emerging hazards, including cyber security risks. The increasing pace of technological and environmental change presents new and highly complex risks for the security and resilience of our critical infrastructure assets, networks and systems. As recent emergencies have demonstrated, our communities are heavily reliant on critical infrastructure for their health, safety and prosperity.

We share the Commonwealth's concern about the increasing risk posed by malicious cyber threat groups, as well as the need to prepare for future advanced threats including cyberterrorism and cyberwarfare. The complex interconnected and interdependent nature of critical infrastructure increases the risk of systemic failure. It is timely that there is further engagement about the critical infrastructure threat environment and the necessary steps required to strengthen mitigation, response and resilient recovery.

While cyber security must be a necessary focus of any future reform, as Victoria's *Critical Infrastructure Resilience Strategy* notes, "the best protection is achieved by improving the resilience of critical infrastructure to all potential hazards, whether natural or human induced." Instead of focusing on the type and likelihood of specific threats, an all-hazards resilience approach better focuses on the likely consequences of a failure of a specific asset, network or other infrastructure component and seeks to mitigate them. Although some residual risk will always be present, risk management strategies can help build capacity for industry and communities to become more resilient to disasters, disruptions and crises. Victoria therefore supports the proposal to align obligations with existing all hazards arrangements.

However, without overarching outcomes and an evidence-base attached to the specific measures, our ability to assess the need, utility and suitability of the overall approach is limited. Critical infrastructure legislative arrangements in Victoria are well established and significantly more mature than those proposed in the consultation paper, so it is unclear how this approach will deliver above and beyond



the baseline already existing in Victoria for many sectors. Victoria offers the following assessment of suitability of the proposed process and various measures based on the information provided and in the limited time available.

The proposed passage of legislation prior to resolving complex implementation challenges presents significant risks. Further detail and consultation will be essential to be able to offer a view on the proposed approach as a whole, whether it will lead to better security and resilience outcomes for infrastructure, and whether it is the most appropriate path for future reform.

3. Defining the Scope and Application of Reform

3.1 Sectors

The Victorian Government welcomes consideration of a broad range of sectors as part of the development of the scheme to ensure all entities of national significance, their supply chains and interdependencies are captured. However, the current list of sectors is not comprehensive or well-defined and it is unclear what evidence has been drawn upon to determine which sectors are in and out of scope.

Our recent experience of COVID-19 has highlighted that during a large-scale emergency, sectors such as manufacturing, chemicals, freight and waste all play critical roles and have high risk interdependencies with other sectors. Victoria would welcome the inclusion of these sectors.

Greater detail is also needed on the scope of the listed sectors and the rationale behind their inclusion to be able to assess the suitability and regulatory impacts of the scheme. A nuanced sub-sector approach would help provide greater clarity and support consideration of the proposal. For example, 'Education, Research and Innovation' could capture a sizable and diverse group of entities. It is unclear whether this descriptor would capture early childhood providers and the skills sector or is simply intended to capture universities.

Similarly, the inclusion of a 'Data and the Cloud' sector could refer to a broad suite of entities. It is unclear whether it is intended to capture the software and services industry group that undertake data processing, internet services, application and systems software, and managed service providers, or whether it is intended to capture broader technology hardware and capital equipment. Victoria would welcome further engagement on the definition and classification of all sectors captured in the reforms.

3.2 Entity Level

Victoria supports the proposed approach to engage with entities across each sector and agrees that a one-size-fits-all approach is not desirable. Many sectors capture entities that are vastly different in their service delivery, size, nature, risk maturity and existing levels of regulation. Different geographies and jurisdictions will also have different threat levels, one size will not fit all even within an industry. Victoria would welcome robust engagement with entities of all sizes to avoid duplication of risk management and regulatory requirements. This will also act to reduce additional, unnecessary and/or disproportionate burden, particularly on small-to-medium enterprises who may not have the necessary financial and/or human resources and access to cyber security services.

Nevertheless, there must be some degree of consistency in the baseline expected across sectors if the intent is to build a baseline of security and resilience across Australia's critical infrastructure. Consistent principles and resulting security requirements and outcomes across sectors will avoid

variances in application and implementation as well as disproportionate regulatory burden on comparable entities within different sectors or entities that operate across multiple sectors. It will also better allow for critical dependencies within supply chains to be captured, acknowledging the interconnectedness of critical infrastructure.

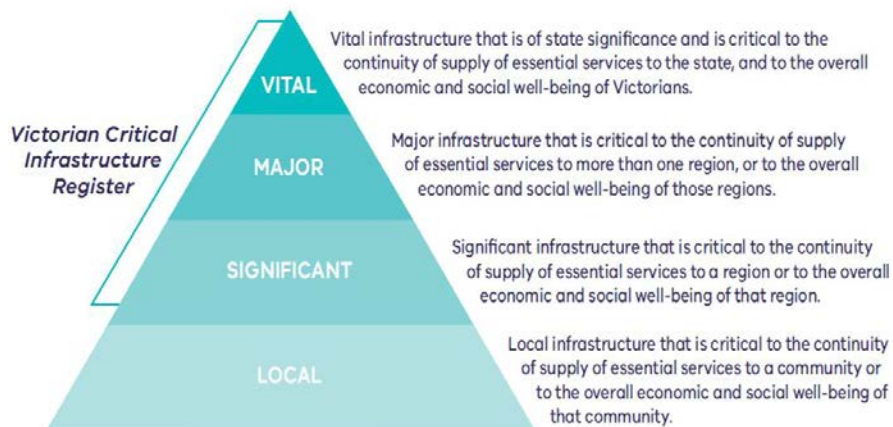
3.3 Defining Criticality

Victoria supports an approach to categorise and prioritise entities to ensure a tailored application of, and compliance with, scalable and risk-based regulations. Victoria proposes that in the first instance, the framework should adopt Victoria's existing critical infrastructure resilience model and approach to criticality assessments and recognise those entities which have already been assessed. This will avoid potential confusion and duplication of effort, as well as ensure consistent use of terminology. This would also apply for the resilience improvement cycle and its compliance and attestation requirements discussed below.

Victoria's assessment model offers a more mature approach, based on an objective assessment of consequence and risk, using a common matrix. The Victorian methodology determines vital critical infrastructure to be infrastructure that, when disrupted, could adversely impact the continuity of the supply of an essential service to Victoria, or the economic or social well-being of Victoria.

The Victorian methodology looks at the services provided, the assets and systems required to support service provision, the key risks, dependencies and consequences of service disruption or asset failure, the population serviced and the strategies in place or redundancies (margin of manoeuvre) to mitigate against key risks.

Figure 1: The Victorian Critical Infrastructure Model



Victoria encourages the Commonwealth to adopt Victoria's approach to ensure consistency and provide clarity to owners and operators and also to capture place-based criticality and risks. This approach would recognise variances in criticality between jurisdictions and address risks accordingly.

4. Delivering Inclusive and Representative Governance Arrangements

Victoria supports the view that building the resilience of national infrastructure is a shared responsibility. The community expects that government will take appropriate measures to ensure owners and operators manage their risks and provide support where required so vital service delivery is not interrupted. However, there is a vital role for all levels of government in strengthening the security and resilience of critical infrastructure, not just the Australian Government.

4.1 State Government

It is unclear from the consultation paper what role State Governments would play beyond consultation and co-design.

State Governments are increasingly a first line of defence in tackling national security and other risks. State Governments are investors, owners, operators and regulators of critical infrastructure as well as the lead on emergency response for all hazards. The viability of reforms therefore relies on State governments having an end-to-end role in designing, implementing and administering the arrangements.

Furthermore, Victoria has identified constitutional limitations on the Commonwealth's ability to legislate in some of the proposed sectors such as transport, health and education. Victoria would welcome further advice from the Commonwealth on how it intends to expand the critical infrastructure legislation to incorporate the reforms and how the constitutional limits of Commonwealth powers will be effectively managed under this proposal. The current proposal risks the creation of different legislative regimes both between and within sectors and consideration is needed on how to address these risks.

The Victorian Government would therefore welcome a revised partnership approach to critical infrastructure reform that recognises the central role of State Governments and constitutional limits on Commonwealth powers, builds on existing State capabilities and arrangements, and supports uplift where the Commonwealth has greater expertise and resources.

Areas where the State Government should have a direct role in the arrangements include:

- Sharing intelligence across the entire supply chain to inform criticality assessments and risk ratings within each sector
- Participating in governance structures to support ongoing implementation including deliberative decision-making bodies
- Sharing expertise to develop sector standards
- Responding to identified emergencies, including cyber emergencies under the Cyber Incident Management Arrangements, drawing on real-time information shared by industry and the Commonwealth
- Undertaking a regulatory role aligned with existing areas to avoid duplication and constitutional over-reach (where appropriate Commonwealth funding can be provided)
- Continuing to support activities to reduce risk consistent with shared commitments under the National Disaster Risk Reduction Framework and drawing on Commonwealth intelligence
- Contributing to advice and decision-making on directives within its jurisdiction.

Neither the Commonwealth nor State Governments will be effective in uplifting capability alone. Only a partnership approach will deliver meaningful and timely strides to improve the security and resilience of critical infrastructure against emerging threats.

4.2 Industry

The Victorian Government supports a review of the Trusted Information Sharing Network (TISN) model and its potential use in future emergency management and response arrangements. The TISN structure has proven to be an effective engagement mechanism between government and industry to share early information regarding risks and to support critical engagement during crises. The use of



TISN throughout the 2019-20 bushfires and COVID-19 pandemic has been highly effective in coordinating industry information and collaboration.

However, the effective uplift and management of enhanced critical infrastructure security obligations will rely on an enhanced TISN model. This will involve bringing new sectors to the table as well as re-engaging sectors, such as transport, which does not currently meet through a centralised forum. Victoria supports the expansion of TISN functions to incorporate stronger engagement, including that of government, state regulators and industry body representatives. The expansion of TISN membership would support the reform goals of government capability uplift and improve information sharing between government and industry.

Whilst Victoria supports the current sector focus, a revised TISN model should allow for cross-sector collaboration and engagement, noting the increased interdependences and supply chain risks that have emerged throughout the COVID-19 pandemic. Victoria would support a tiered collaboration model that engages entities in deliberative decision-making and consultation relevant to risk.

Victoria also notes the important role for Australia's cyber security industry. There would be significant value in the industry having an active voice in new governance arrangements and offering improved support measures to help the industry assist organisations in meeting their new obligations.

5. Developing targeted obligations and supports

5.1 Positive Security Obligations

Victoria supports-in-principle the proposed outcomes for positive security obligations to mitigate and manage risks that may impact critical infrastructure. Victoria notes that the obligations relate specifically to security risks (personnel, protective security and cyber) and queries whether these are sufficiently broad to support the all hazards framework outlined at the start of the submission.

Victoria supports-in-principle strengthening visibility and risk management of supply chains but notes that critical infrastructure sectors within Australia often lack the market power to influence global suppliers. In an increasingly globalised world, arrangements need to recognise the limits of industry influence and look at alternative options to address risk and resilience, such as working to strengthen international standards or build local capabilities.

Victoria also cautions against the potential for duplication with prescribed arrangements under part 7A of the *Emergency Management Act 2013* (Vic). In Victoria, critical infrastructure entities are already required to complete a Statement of Assurance if declared to be vital to the State of Victoria. Currently, critical infrastructure owners and operators in the energy, water and transport sectors are subject to these requirements. Any further requirements under the proposed Positive Security Obligation may disproportionately increase the administrative and cost burden on critical infrastructure entities in Victoria and on their customers. Proposed legislation should provide clear guarantees that any existing Victorian government legislation can be taken as sufficient to meet the proposed obligations or that, at a minimum, specific elements be deemed sufficient.

Victoria also deems that there is a critical need for State regulators to develop sector standards, thresholds and guidance for critical infrastructure providers to ensure consistent cyber security uplift across sectors. The regulatory regime is discussed further at section 6.

5.2 Enhanced Cyber Security Obligation

In recognition of the need to build cyber security capability and understanding of threats, the Victorian government is supportive of the need to undertake enhanced cyber security activities, including the development of a playbook of response plans. In order to accurately determine roles and responsibilities, Victoria considers that playbooks should include, but not be limited to, incident thresholds, contact lists, practical step-by-step guidance for entities to follow, and specific advice for executives to act on. Playbooks must also recognise the existing incident response arrangements at the state level, as well as those established within specific sectors, and maintain an 'outcome based' approach to ensure they remain relevant to the changing threat landscape. Current experience shows that exercising playbooks is just as important as developing them, therefore Victoria would support exercises undertaken in partnership with response agencies to strengthen response arrangements.

Information and intelligence sharing

In addition to the preparatory activities outlined in the discussion paper, Victoria would also support enhanced information and intelligence sharing between government and industry, the establishment of a common risk and vulnerability assessment framework and the inclusion of joint exercising as described above. In doing this, consideration should also be given to existing sector-specific cyber security frameworks and information sharing arrangements such as the Australian Energy Market Operator's (AEMO) Australian Energy Sector Cyber Security Framework.

Victoria recognises the increased need to proactively identify and remediate cyber vulnerabilities, however this information must be shared in a timely manner across industry and all levels of government to limit duplication of effort, enable the effective management of risk and support response arrangements. Victoria considers that the following cyber information should be shared to reduce vulnerabilities: assessments of cyber maturity against recognised frameworks, strategic cyber priorities; cyber threat intelligence; a national cyber incidence response framework and emergency contact information.

However, information sharing should not be limited to cyber risks. Increased sharing of threat information across all hazards will enable greater industry preparedness and reduce the duplication of efforts across industry and sectors. Two-way information flows will also assist States in making informed decisions regarding threats, risk reduction, policy, investment and regulation, and increase understanding about interdependencies and supply chains. Information sharing is critical to any proposed reform or model for critical infrastructure security.

Furthermore, information and intelligence sharing will assist with response activities in the event of a significant emergency, such as widescale cyber threats. Victoria notes the Commonwealth may not have the capacity to provide dedicated resources to protect critical assets outside of the Australian Government and will rely on States and Territories in these situations. The viability of Victoria's emergency response will depend heavily upon two-way information flows.

Data security

Across all elements of the enhanced cyber security obligation, the security of data is paramount and should be protected through safeguards and assurances. At a minimum, the Victorian Government would expect data to be disposed of when no longer required, the right to correct, confidentiality across all domains and the establishment of a framework on the use or release of all data provided. Ongoing industry and state engagement is reliant on clear, established data safety protocols and assurances.

5.3 Cyber Assistance for Entities

A clear expectation needs to be set that entities will be responsible for management of their risks, including cyber, and that possible government assistance is not a reason to undertake minimum or inadequate resilience activity on the basis that they can rely on the government to step in and remedy the situation. The situations in which the Australian Government can actively intervene should be clearly identified.

The Victorian Government considers that cyber assistance for entities should only be activated when the consequence of a cyber-attack on critical infrastructure is deemed critical to Australia's economy, security or sovereignty or represents an imminent threat to life. Victoria's position on the declaration of an emergency (and the roles and responsibilities of industry and the State) in accordance with cyber security is outlined in more detail below.

6. Establishing a Best-Practice Regulatory Model

6.1 Regulators

The current proposal would be strengthened by clarifying how the critical infrastructure reforms will be regulated. Victoria would welcome further information on the proposed regulators, the proposed number of regulators and/or the use of current regulatory bodies including State regulators. Victoria also asserts that the role of the regulator(s) will be significant and queries the feasibility of a single Commonwealth regulator.

6.2 Regulatory Burden

There is already a complex regulatory environment at the State and Federal level for critical infrastructure entities. The overlay of additional frameworks may create considerable confusion and lack of clarity about roles and responsibilities in relation to critical infrastructure, cyber security and the management of cyber and other emergencies. As there is limited detail regarding 'sector standards', Victoria notes the proposed model could potentially duplicate existing legislative requirements and standards at four levels:

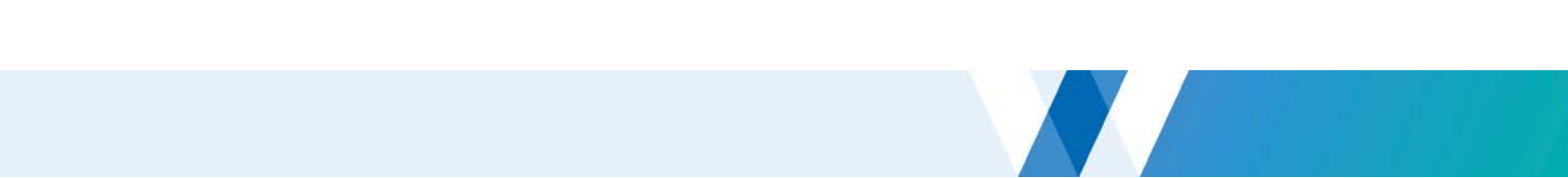
A) Victoria's emergency management and critical infrastructure arrangements

Under Part 7A of the *Emergency Management Act 2013*, owners and operators of critical infrastructure deemed vital to the State's interests have legislated responsibilities to undertake annual attestations, emergency management planning, exercises and audits.

B) Sector regulatory models

Each sector has complex layers of existing governance and regulatory oversight. For example, in Victoria in the water sector, entities are subject to Ministerial and parliamentary oversight on business performance including performance against government security and resilience policy. They are also subject to specific obligations in areas such as service delivery, asset management, dam safety, risk and emergency management under the *Water Act 1989 (Vic)*, the *Water Industry Act 1994 (Vic)* and Statements of Obligations in addition to the duplication outlined at points A and C.

In an entirely privately owned and operated sector such as the Banking and Finance sector, Victoria observes that Banking and Finance entities are already strictly governed and regulated by sector specific legislation and are also subject to a range of general obligations under Corporations Law. There are also substantial regulatory obligations to other regulators such as the Reserve Bank of Australia and the Australian Prudential Regulation Authority in matters proposed under the critical



infrastructure reforms. Any new critical infrastructure legislation should reflect existing arrangements and ensure clarity and alignment of roles and responsibilities across Commonwealth regulators. Victoria would welcome a more detailed gap analysis covering existing regulation to support the case for further regulation across all sectors.

C) Government Risk Management and Cyber Security Frameworks

As detailed above, some critical infrastructure entities are owned or operated by State Governments. Capturing these entities will increase the risk of duplication with existing risk management models for public sector entities and their obligations and accountabilities to Ministers. In Victoria, the Victorian Government Risk Management Framework and the Cyber Security Strategy set clear obligations on entities to meet security and resilience measures. Oversight is established via parliamentary processes, independent audits and independent regulators such as Office of the Victorian Information Commissioner.

D) Data security and privacy obligations

Victorian critical infrastructure entities are also subject to a suite of data security and privacy requirements which regulate the collection and handling of personal information such as the *Privacy and Data Protection Act 2014* (Vic) and the *Health Records Act 2001* (Vic). Any proposed model should conform to these requirements to avoid duplication of existing arrangements.

6.3 Standards

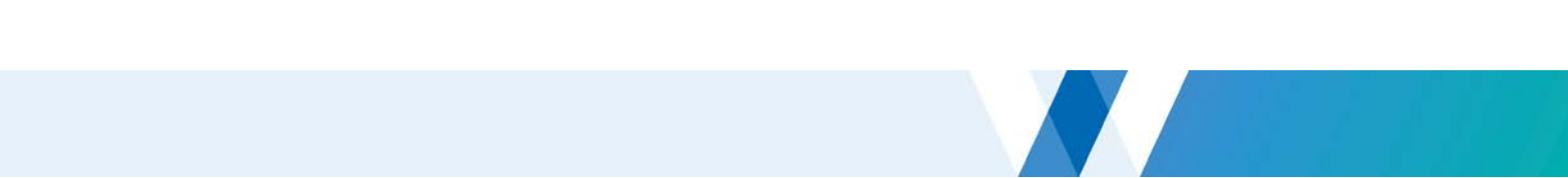
The proposal would be strengthened by clarifying who will set standards and how consistency will be achieved given the sector-specific focus proposed. Similarly, it would be helpful to identify who will update and develop supporting material for the standards. While Victoria recognises the varying levels of maturity within and between sectors, devolving standard development to sector-specific regulators may lead to the inconsistent development and application of standards. It will also likely result in missing interconnections between sectors and create inconsistencies throughout supply chains. Inconsistent application of standards will lead to reduced security outcomes and challenge effective enforcement and governance of the reforms. Victoria would welcome standards based on criticality that build on the collective expertise of existing sector regulators.

Achieving alignment of standards to security best practice and consistency across sectors will ultimately lead to greater levels of protection to critical infrastructure, whilst reducing the burden on industry and regulators. Victoria supports the further joint examination of a common tiered maturity model based on asset criticality, rather than asset type, underpinning any specific sector-based standards. A common tiered criticality-based standard would further align the reforms to existing international standards.

Standards will also need to be regularly updated. The pace of technological, economic and environmental change creates a complex risk environment. Standards will need to be constantly evolving and regulation will need to be able to be readily adjusted based on learnings to prevent repeated interventions.

6.4 Compliance and Enforcement

For an effective enforcement regime, adequate information and guidelines will need to be provided to owners and operators, clearly articulating their responsibilities. The existing timelines are challenging and would not enable this to occur, potentially setting owners and operators of critical infrastructure up for failure and breach of legislation. The timelines are compounded by the cyber skills gaps – the very challenge identified in the recent Australian Government Cyber Security Strategy. This will



further impact the ability of operators and regulators to implement, comply with and enforce any proposed obligations. The viability of any reforms will necessarily depend upon a longer-term outlook for reform. The Victorian Government would not support an AusCheck style scheme for personnel registration and security checks without a clear evidence base outlining the need and a thorough understanding of industry impacts. Instead, Victoria would welcome an approach that looks to identify the most critical and vulnerable roles rather than take a blanket approach to sectors or systems.

Recognising the scope of the proposal and the intent to capture State-owned critical infrastructure, a dispute resolution mechanism, satisfactory to State Governments, should also be incorporated. The introduction of a dispute resolution mechanism would ensure greater transparency and accountability within the proposed model and promote ongoing cooperation between government and entities.

6.5 Cost burden

The proposed reforms introduce potentially significant financial and administrative burdens on entities without federal funding. For many regulated sectors, the proposed changes have not been considered as part of recent price submissions. It is likely that costs will need to be passed on to consumers and end users at a time of significant economic downturn and reduced household incomes. Where costs cannot be passed on, the reforms may have unintended consequences for investment and sector growth. Costs of security clearances and maintenance of security regimes will be ongoing, making it difficult to quantify immediately. A Regulation Impact Statement is essential to ensure these costs are considered and will support States in identifying and minimising duplication.

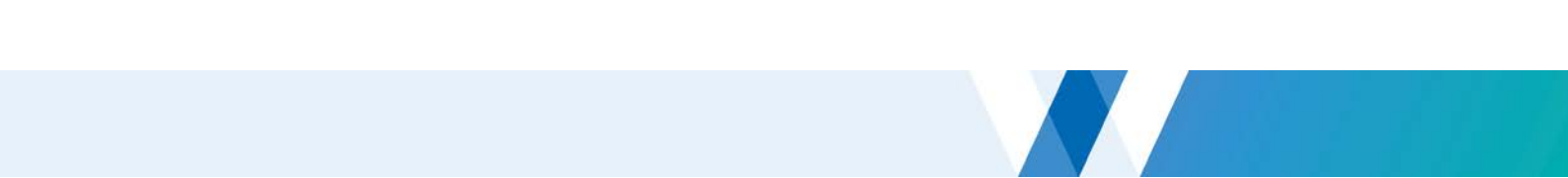
In addition to the cost burden on industry and customers, there are clear cost burdens involved for state and territory governments in supporting the Commonwealth to build a tenable national critical infrastructure regime. These costs will be exacerbated if the regime is poorly designed. Any proposed amendments will need to be adequately resourced and funded, at both the State and Commonwealth level. It may be worth consulting with Defence on their industry security program to consider how their costs are defrayed, noting that most Defence contractors are advised prior to tendering that costs will be associated with meeting security requirements, rather than being retroactive as will occur with this legislation.

7. Establishing Appropriate and Proportionate Commonwealth Powers

7.1 Declaration of an emergency

The Victorian Government does not support the Commonwealth proposal to introduce a new concept of a 'declared emergency' even where there is a threat to Australia's economy, security or threat to life. Victoria considers that existing federal mechanisms are adequate and appropriate for facilitating intergovernmental cooperation in response to all emergencies, including cyber emergencies, and the proposed changes will likely generate poor security outcomes. Furthermore, it is unclear what value add this declaration would bring to security and resilience given existing directions powers are already available to Ministers under the *Security of Critical Infrastructure Act 2018* (Cth) (SOCI Act).

The Victorian Government has provided an extensive submission on the constitutionality and implementation challenges associated with a declaration of a national emergency to the Royal Commission into National Natural Disaster Arrangements. While this was specific to natural disasters, the issues and implementation challenges are similar. The proposal for a Commonwealth declared emergency is extremely problematic given existing legislative State emergency management responsibilities and obligations in managing emergencies across all hazards.



Under Victoria's existing legislated emergency management obligations, the State has clear accountabilities for responding to emergencies including cyber emergencies, managing consequences and supporting recovery across the economic, social, built and natural environments. Victoria, through its Sector Resilience Networks, has developed strong and trusted working relationships with industry, which provide the necessary information flows and contacts to respond in a timely and coordinated way to identified emergencies.

Creating new arrangements for a nationally declared emergency may impede the States' response and create confusion in times of emergency. In the context of cyber emergencies for example, Victoria notes that the Commonwealth's emergency role specifically relates to matters of sovereignty and security rather than domestic criminal activity or human and technological error. The motivation or origin of the cyber incident will not always be clear, making thresholds for the proposed provision problematic. There would be a risk that action will not take place or action will be duplicated by both levels of Government. Victoria urges the Commonwealth to ensure that the proposed reforms are designed so that there are still clear control arrangements during an emergency.

Further consideration should also be given to how the proposal would support control arrangements during concurrent emergencies. As all States and Territories operate in an all hazards environment, it would be counterproductive to have two competing control arrangements. Not only would this risk inefficient use of limited emergency management resources, but it also risks producing poor outcomes for industry and community who experience compounding impacts and consequences.

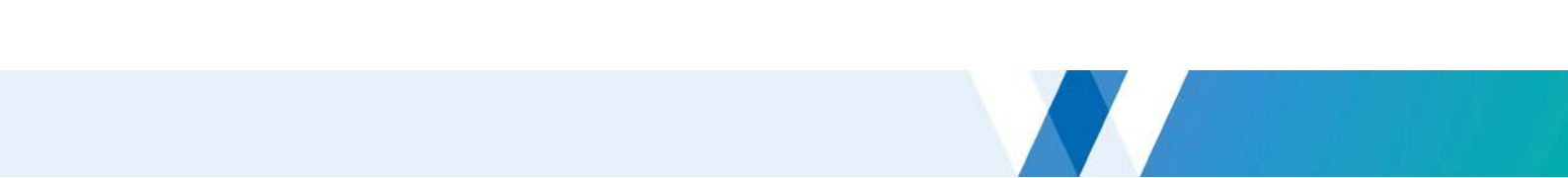
Instead, Victoria recommends exploring options to better leverage State arrangements and support State response and recovery efforts with their expertise and resources, particularly in relation to cyber security.

7.2 Ministerial directions power

The Victorian Government recognises that the relevant Commonwealth Minister already has power to direct a responsible entity to take action to mitigate an assessed national security risk. Under the current SOCI Act, the exercise of the Ministerial direction power requires consultation with the relevant state and territory minister in which the critical infrastructure asset is located. Victoria considers that this should continue to be a cornerstone of the regime moving forward to avoid both the duplication of action and the failure to act where there is ambiguity in roles or responsibilities.

However, state-owned and operated assets should be explicitly exempt from the Ministerial directions power. Victoria believes that a Ministerial direction power that applies to critical infrastructure assets that are both owned and operated by the state would unnecessarily impact state sovereignty. Instead the Commonwealth should inform relevant state ministers of the national security risk to a state owned and operated critical infrastructure asset and work with the state to effectively mitigate the threat. For a state owned and operated asset, a state minister has the power to issue directions to a responsible entity in relation to the performance of any of its functions or the exercise of any of its powers. Therefore, it would not be appropriate for the Commonwealth to intervene, even in the extremely unlikely instance where a state refuses to act to mitigate a security threat. Ultimately, decisions regarding the functions of state owned and operated critical infrastructure assets should remain a matter for the states.

Victoria also notes that the proposed interventions may pose risks to capability uplift. Consideration will need to be given to managing the risk that an increased Commonwealth role may promote underinvestment in cyber security due to the perception of a Commonwealth safety net. There may



also be increased levels of risk to industry should the Commonwealth direct action that will result in collateral or additional damage to critical infrastructure. The proposed reforms will need to be designed to ensure business level risk is not transferred to government through a prescribed approach.

7.3 Transparency, oversight and safeguards

Any Commonwealth powers must have an independent oversight process to provide assurance that the use of powers has been appropriate and proportionate to the circumstances. Regular public reports to parliament on the application of the scheme, use of powers and monitoring and evaluation against agreed measures and outcomes will assist with transparency and ensure arrangements remain fit for purpose. This will, however, need to minimise the reporting burden on industry and leverage existing arrangements.

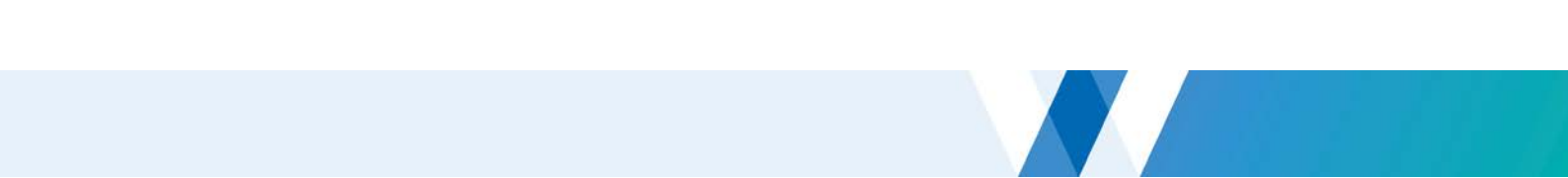
Various safeguards will also be needed as part of the regime, noting the significant potential privacy and security implications. Compliance with relevant Australian and international privacy legislation, such as the European Union's General Data Protection Regulations, will be required to protect privacy and ensure industry viability. Loss of control of business and customer data to other parties is a significant concern, and the arrangements would be strengthened by setting out requirements for any data obtained directly or indirectly via these arrangements to be disposed of when no longer required.

8. Concluding Remarks

The Victorian Government welcomes the opportunity to provide further input during sector-specific consultation and co-design, to help refine, shape and progress the framework for the economic and social benefit of communities serviced by these sectors. Victoria supports the proposed capability uplift across physical and cyber security in critical infrastructure sectors, however the consultation paper does not provide sufficient detail to support the proposed process and implementation. Further, the indicative timelines are both restrictive and do not allow for adequate industry consultation, thereby limiting the ability of critical infrastructure sectors to engage with and adapt current frameworks to support the reform.

The proposed reforms and intended uplift across critical infrastructure sectors must be supported by a clear end-to-end role for State Governments. Currently, the role of States is not defined and risks excluding States from arrangements. As owners, operators, investors and regulators of critical infrastructure, states are best placed to lead emergency responses and facilitate enhanced security and resilience. Further, the role of the Commonwealth is not clearly defined within the proposed reforms. The proposed reforms do not identify how the Commonwealth will overcome constitutional limits to enforce enhanced physical and cyber security obligations within sectors which it does not currently regulate.

Based on the available information Victoria also identifies that there is a significant risk that the proposed model does not fully reflect best-practice standards and will increase regulatory burden and cost, overwhelming industries already subject to State, sector-specific and Commonwealth legislation. Victoria would urge the Commonwealth to recognise and leverage the existing state-based regulatory arrangements already in place in Victoria. Leveraging existing arrangements, such as Victoria's critical infrastructure arrangements, would avoid duplication and provide a more streamlined approach, minimise regulatory burden and reduce the cost impact on states, industry and consumers.



Two-way information and intelligence sharing will also be vital to ensuring the proposed reforms deliver sustainable and effective uplift across critical infrastructure and will support inclusive and representative governance arrangements. In coordination with robust and independent oversight and safeguards, two-way information sharing will establish strong partnerships to promote and enhance the security of Australia's critical infrastructure sector.

Greater consultation and engagement with all levels of government and industry prior to the passage of legislation will enable the co-design of a more deliberative national critical infrastructure regime that can balance security and resilience outcomes with the need for ongoing investment and sector growth.