CYBER SECURITY
COOPERATIVE
RESEARCH
CENTRE

# SUBMISSION:

## Protecting Critical Infrastructure and Systems of National Significance

cybersecuritycrc.org.au

Dear Sir/Madam,

**Submission: Protecting Critical Infrastructure and Systems of National Significance**

I am pleased to submit the Cyber Security Cooperative Research Centre's (CSCRC) response to the Department of Home Affairs regarding its *Protecting Critical Infrastructure and Systems of National Significance* consultation paper. We commend the Federal Government for its ongoing commitment to ensuring Australia remains a safe and secure nation, one well-equipped to meet the challenges of the digital age through the daily delivery of essential services to millions of Australians.

**About the CSCRC**

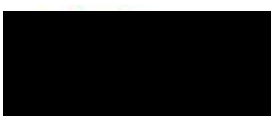
The CSCRC is dedicated to fostering the next generation of Australian cyber security talent, developing innovative projects to strengthen our nation's cyber security capabilities. We build effective collaborations between industry, government and researchers, creating real-world solutions for pressing cyber-related problems.

By identifying, funding and supporting research projects that build Australia's cyber security capacity, strengthen the cyber security of Australian businesses and address policy and legislative issues across the cyber spectrum, the CSCRC is a key player in the nation's cyber ecosystem. The CSCRC has two research programs: Critical Infrastructure Security and Cyber Security as a Service.

The CSCRC is a public company limited by guarantee and will invest $AU50 million of Australian Commonwealth Government funding and additional Participant funding over seven years to 2025 in research outcomes related to our key impact areas. The CSCRC has 25 Participants including seven Research Providers, eight State and Federal Government Agencies/Departments and 10 Industry/SMEs.

We look forward to answering any queries about this submission and welcome the opportunity to participate in future consultation rounds regarding this very important topic.

Yours Sincerely,



Rachael Falk
CEO, Cyber Security Cooperative Research Centre
[redacted]

## Executive Summary

The Cyber Security Cooperative Research Centre (CSCRC) welcomes the opportunity to provide this submission to the Department of Home Affairs in response to the release of its August 2020 consultation paper, *Protecting Critical Infrastructure and Systems of National Significance*. The consultation process is timely and pertinent given the escalating cyber threat environment and the increasingly networked nature of Australia's critical infrastructure in the digital age.

In recent years, there have been a spate of high-profile attacks on critical infrastructure networks around the globe. The 'Nuclear 17' hack on nuclear facilities in the United States in 2017 ultimately inflicted no significant damage to the critical infrastructure network. It did, however, highlight the network's vulnerabilities to future, potentially catastrophic attacks. In May this year, the United Kingdom's electricity grid suffered a cyber attack on its IT infrastructure. Existing cyber security measures proved robust enough to maintain continuity of electricity supplies to residents but the warning was clear.

Australia is not immune to this nefarious cyber activity. On 19 June 2020, Prime Minister Scott Morrison issued a public statement noting sustained malicious cyber activity was being directed at Australian networks, including critical infrastructure and essential services providers. Australian businesses were urged to take immediate measures to bolster their cyber security resiliency.

Critical infrastructure – the functions and services that facilitate our everyday lives – underpins almost everything we do. Almost all the networks and systems relied on by critical infrastructure entities run on digital communications, some of which are not cyber secure and remain vulnerable to cyber threats. Strategic disruption to critical infrastructure and supply chains remains a substantive catalyst for threat actors, with potentially catastrophic effects for economies and society alike.[1] The pivotal stance taken by Federal Government to ban Huawei from Australia's burgeoning 5G network indicates the gravity and scale of potential risks involved.

The consultation paper highlights the vital importance of securing our essential services in the digital age. It is imperative that during a period of rising malicious cyber activity globally, owners and operators of essential networks are equipped with the appropriate measures to adequately prepare for and respond to the rapidly evolving threat landscape.

[1] https://harvardnsj.org/wp-content/uploads/sites/13/2016/06/Carlin-FINAL.pdf, p. 398.

This consultation process offers a clear opportunity for Australia to ensure that our most essential services are effectively safeguarded against physical and cyber security threats. We are already world leaders in this regard – the Australian Government took the step of enshrining a definition of 'critical infrastructure' in legislation in the *Security of Critical Infrastructure Act 2018*. The proposed next steps will only enhance Australia's reputation as a nation at the forefront of efforts to safeguard its citizens and critical systems.

Our submission responds to the following:

**1. Do the sectors above capture the functions that are vital to Australia's economy, security and sovereignty? Are there any other sectors that you think should be considered as part of these reforms (e.g. manufacturing)?**
**&**
**2. Do you think the current definition of Critical Infrastructure is still fit for purpose?**
Considering these two issues together, the CSCRC commends the Federal Government for the proactive actions taken to secure Australia's critical infrastructure and essential services providers. The consideration, inclusion and expanded definition of Australian critical infrastructure providers is adequate and suitably broad. The CSCRC notes the expanded definition now captures a much larger segment of the economy and it will help to ensure the future security of Australia's critical infrastructure and national security. It also mirrors a key recommendation made in the *Industry Advisory Panel Report* into Australia's 2020 Cyber Security Strategy, which stated the definition of critical infrastructure should be expanded to capture "all essential services and functions in the public and private sectors", which should operate under "consistent, principles-based regulatory requirements to implement reasonable protection against cyber threats".[2]

This expanded definition is timely. In recent months we have witnessed cyber attacks on Australian organisations which supply critical and essential services. In May 2020, BlueScope Steel, the Australian steel maker, suffered a crippling ransomware attack that severely impacted the company's global operations. The attack had far-reaching impacts, upsetting operations at the Port Kembla plant in NSW. In June 2020, Australia's largest brewing and dairy manufacturer, Lion Dairy and Drink, suffered a cyber attack which disrupted its entire supply chain and forced the drinks giant to halt production.

[2] https://www.homeaffairs.gov.au/cyber-security-subsite/files/2020-cyber-security-strategy-iap-report.pdf, p. 7

Furthermore, the COVID-19 pandemic has witnessed a rise in malicious cyber activity across organisations that now fall under the expanded definition of critical infrastructure providers, most prominently in the healthcare space. On 17 July 2020 relevant Australian Government agencies issued a joint statement demonstrating their support of the publication of the UK-US-Canada Joint Cyber Security Advisory. The advisory outlined recent and sustained cyber-espionage activity by Russian cyber actors to exploit the global pandemic and gain unauthorised access to COVID-19 vaccine research. Russia was strongly urged by the Australian Government to not renege on its commitments to international cyber norms and conventions.

Considering the heightened threat environment, the CSCRC notes the existing definition, with an increased scope, is fit for purpose. The crucial distinction in the definition of both 'physical facilities' and 'information technologies and communication networks' renders activity in both the offline and online worlds of equal significance. Furthermore, the expansion of the definition will only serve to enhance the cyber security posture of Australian sectors, contributing to a critical uplift across the entire economy.

**7. How do you think a revised TISN and Critical infrastructure Resilience Strategy would support the reforms proposed in this Consultation Paper?**

**&**

**9. How else should government support critical infrastructure entities to effectively understand and manage risks, particularly in relation to cross sector dependencies? What specific activities should be the focus?**

Concerning the revised TISN and Critical Infrastructure Resilience Strategy, the CSCRC contends these measures will serve to enhance reforms across the Australian critical infrastructure ecosystem. Bolstered mechanisms to enhance communications, trust and sharing of threat intelligence about physical and cyber threats will continue to provide practical opportunities for owners and operators to solidify their understanding of the threat environment. To achieve maximum impact, any sharing mechanism in this capacity should ensure that information is shared in a timely manner with useful insights for relevant stakeholders and their businesses. This will enhance mitigation strategies and strengthen the resiliency of Australia's critical infrastructure.

Concerning opportunities for government to support critical infrastructure entities to effectively understand and manage risks, the CSCRC urges ongoing and real-time threat and vulnerability sharing with industry partners. This is particularly important as it comes to understanding downstream and upstream supply chain risks and the cascading effects a cyber breach could trigger.

Another key component of this support includes underscoring to entities across all sectors their systemic reliance on digital systems – the ubiquitous communications backbone on which their networks run – and the shared responsibility cyber uplift entails. The globally interconnected nature

of these communication networks remains, at all times, vulnerable to cyber security threats. Accordingly, support and uplift activities offered by government should emphasise the critical importance of cyber security and the 'secure by design' principle. Lastly, the CSCRC recommends the harmonisation of communication with critical infrastructure providers and the provision of clear guidance on 'how' this support will occur and what it will entail.

**10. Are the principles-based outcomes sufficiently broad to consider all aspects of security risk across sectors you are familiar with?**

The CSCRC finds the principles sufficiently broad concerning relevant sectors our organisation has familiarity with and commends the Federal Government for presenting succinct principles-based outcomes. These principles take a welcome proactive approach to security, offering a simple framework which can be built upon by companies at the implementation stage. Furthermore, in the interests of harmonisation, these outcomes also correlate well with the Australian Cyber Security Centre's (ACSC) *Essential Eight*.

Nonetheless, the CSCRC urges further consideration of how to update these principles in line with pertinent and real-time security developments. This remains an ever-present challenge particularly in the cyber domain, and accordingly, the CSCRC suggests these principles be subject to annual review and updated to capture any significant changes in the security risk environment.

**16. The sector regulator will provide guidance to entities on how to meet their obligation. Are there particular things you would like to see included in this guidance, or broader communication and engagement strategies of the regulator?**

**&**

**18. What kind of support would be beneficial for sector regulators to understand their additional responsibilities as regulators?**

The CSCRC supports the proposed efforts by the sector regulator to provide guidance to entities on how to meet obligations. In that regard, we recommend clear communiques regarding cyber security risks and obligations, including ongoing advisories from the sector regulator.

The request for sustained communication is pertinent considering fast-moving developments in regulatory requirements, of which relevant entities may not be informed. In August 2020, the Australian Security and Investment Commission (ASIC) commenced proceedings against RI Advice Group (RI) under s912A of the *Corporations Act 2001* (Cth), alleging the company had deficient cyber security controls. Between 2016 and 2020, RI experienced numerous cyber breaches across its networks, although the claims relate to the period from May 2018. ASIC alleges from that point in time, RI had reneged on its duties and obligations to respond to and remedy the known incidents, resulting in an unacceptable level of risk exposure to future cyber security incidents.

This is the first case of its kind launched by ASIC. It has the look and feel of a test case and the potential to set landmark precedent. The case is also significant because the action has been brought by ASIC as opposed to the Office of the Australian Information Commissioner (OAIC), which signals a move towards tougher enforcement in relation to cyber security responsibilities for organisations. Further to this, guidance on which regulators will have oversight and how lines of authority will function, in practice, is advisable. Lastly, the courts' findings in relevant cases should be regularly communicated to all critical infrastructure entities to demonstrate the tangible impacts and consequences cyber security incidents can bear on their operations.

On the latter question, enhanced knowledge about the cyber security threat environment and related risks, at both the macro and micro level, would be beneficial for sector regulators. Achieving this could potentially entail regular briefings and communiques to sector regulators from cyber security domain experts. Clear and prescriptive guidelines will also assist regulators in clarifying both the scope and remit of their increased responsibilities. Presently there are multiple standards which, for boards of critical infrastructure entities, could lead to confusion as to what 'best practice' could be. For example, for financial services critical infrastructure entities regulated by the Australian Prudential Regulation Authority (APRA), there is CPS236 [Prudential Standard CPS 234 Information Security]. For critical infrastructure energy providers, the relevant regulator, Australian Energy Market Operator (AEMO) has set required minimum standards. The CSCRC submits that some level of guidance for boards and management as to their obligations regarding cyber security governance is required, otherwise they could become unnecessarily distracted as to which governance and operational standards to adopt.

**19. How can Government better support critical infrastructure in managing their security risks?**

The CSCRC suggests support come through the following mechanisms: pertinent and timely information about the ever-evolving cyber security threat landscape; clearly defined and prescriptive guidelines; and an ongoing commitment to transparency and threat intelligence sharing. Perhaps most critically, hands-on assistance with the implementation of guidelines and obligations should be considered, given the technical expertise and resource requirements necessary to thoroughly mitigate large enterprises from cyber security threats. Furthermore, as noted in Australia's recent *2020 Cyber Security Strategy*, Australia has a critical skills shortage of cyber security professionals and there is a pressing need to build a holistic pipeline of cyber security talent. Considering this skills gap, government support in this capacity should be immediate and active, with a focus on implementing agreed accreditation standards for Australian cyber security professionals.

**21. Do you have any other comments you would like to make regarding the PSO?**

The CSCRC is supportive of the Federal Government's efforts to create positive security obligations for critical infrastructure providers. The effects will be consequential for our nation and our national security, with significant flow-on effects for all Australian organisations and residents. Positive security obligations will provide clarity for businesses captured by this obligation and help facilitate uplift more generally across the economy. Such obligations also reinforce that cyber security must be a key consideration for businesses in today's world and that complacency is not an option. Ultimately, the introduction of such obligations are demonstrative of the Federal Government's commitment to ensuring Australia remains a global standards-bearer in cyber security and a safe and trusted place to do business.

**22. Do you think there are other preparatory activities that would assist in proactively identifying and remediating cyber vulnerabilities?**

**&**

**23. What information would you like to see shared with industry by Government? What benefits would you expect from greater sharing?**

Considering the first question, the CSCRC's overall recommendation is that preparatory activities, by and large, commence as soon as possible to trigger a cyber uplift across Australia's critical infrastructure and essential services. The CSCRC also encourages government's promotion of mechanisms and measures proven to be effective at bolstering the cyber security posture of businesses, including exercises such as regular penetration testing.

Lastly, the CSCRC notes that in November 2019, the Australian Cyber Security Centre hosted a national cyber security exercise series in collaboration with a select group from across Australia's electricity industry and government agencies, both at the federal and state level. These exercises were designed specifically with potential cyber incidents in mind. While commendable, similar preparatory events should be expanded and offered to all critical infrastructure providers in the future on a regular basis.

Regarding preferred information, the CSCRC encourages the government's commitment to greater transparency and sharing of timely and relevant information about pertinent security threats, cyber included. It comes hand-in-glove with numerous positive benefits which will assist in securing our nation for an increasingly interconnected future.

The CSCRC recommends that government regularly communicate with industry regarding a potential transition period, whereby relevant critical infrastructure entities will be able to take adequate preparatory measures to ensure compliance with coming regulation. An adequate transition period is advisable and prudent given the significant uplift that may be needed across some sectors. We encourage a consideration of the *General Data Protection Regulation* (GDPR), perhaps the most

globally consequential regulatory development in recent years regarding data, adopted by the European Union in 2016. However, its provisions were not required to be fully implementable by all Member States until a full two years later, in May 2018.

**27. What information would you like to see included in playbooks? Are there any barriers to co-developing playbooks with Government?**

Playbooks offer excellent guidance to organisations before, during and after a cyber security incident. They establish clear roles and responsibilities across all members of critical infrastructure providers regarding cyber security, as well as ensuring critical continuity of communications with the board in case of a security incident. Regarding the development of relevant playbooks developed in collaboration with government, the CSCRC notes there are often barriers for organisations to disclose a cyber security breach, including concerns about reputational damage, harmed market confidence and fear of 'tipping off' cyber attackers. The unfortunate by-product of this widespread reticence is that it may be challenging to obtain usable case studies, considering existing concerns around confidentiality and intellectual property. Such an effect could be counteracted by leveraging international relationships – for example engaging with Five Eyes partners – to co-develop playbooks using offshore examples.

**32. If, in an exceptional circumstance, government needs to disrupt the perpetrator to stop a cyber attack, do you think there should be different actions for attackers depending on their location?**

**&**

**34. What safeguards and oversight measures would you expect to ensure the necessary level of accountability for these types of powers?**

COVID-19 has underscored the interconnected nature of our digital world. Large organisations, including critical infrastructure providers, are finding it more challenging to secure networks and prevent cyber threats with wide swathes of the Australian population now working from home under less cyber secure working conditions. Cyber criminals – both offshore and domestic – are acutely aware of this and have been actively seeking to exploit the increased threat surface.

Considering this, different jurisdictional provisions will apply to cyber attackers, according to their location. Attacks launched domestically will be targeted by the appropriate domestic agencies and dealt with accordingly under Australian law.

Offshore perpetrators will fall under the remit of the Australian Signals Directorate (ASD). On that front, the Morrison government, on 30 June 2020, announced a decade-long investment in cyber security capability, the *Cyber Enhance Situational Awareness and Response* (CESAR) package. Billed as Australia's largest ever dedicated contribution to cyber security, the expenditure has been designed to provide a critical boost to the nation's cyber capabilities and aid efforts to thwart rising cyber security threats. Included in this is an augmentation of ASD's offensive cyber security

capabilities, to reinforce their efforts to 'actively disrupt' overseas malicious cyber activity and protect Australia's interests. These strengthened capabilities will adhere to and continue to promote international cyber norms for responsible behaviour in cyberspace. To that end, the CSCRC recommends the Federal Government continue to remain a vocal advocate for cyber deterrence policies and processes to de-escalate global cyber tensions.

Oversight mechanisms should be clearly articulated and mandated in legislation, with appropriate safeguards built in. The recently launched 2020 Cyber Security Strategy has proposed new legislation in this regard, which is forthcoming. This also reflects the recommendations of the *Industry Advisory Panel Report*, which states that malicious actors should be held accountable "via enhanced law enforcement, diplomatic means, and economic sanctions or otherwise as appropriate".[3] The CSCRC has every confidence any oversight mechanisms will cement appropriate democratic checks and balances into this process.

**35. What are the risks to industry? What are the costs and how can we overcome them? Are there sovereign risks to investment that we should be aware of?**

**&**

**36. Does this mix of obligations and assistance reflect the roles and responsibilities of Government and industry in protecting critical infrastructure? How would private sector management of risk change with the proposed increased role for Government?**

Considering these two issues together, industry bears a double-barrelled risk. First, mitigating the potential for foreign interference in Australia's most critical services and second, protecting the sovereignty and national security of our nation while ensuring the continued economic interests of Australia. The recent decision to deny China's Mengniu Dairy Co's acquisition of Lion Dairy and Drink is case in point of the balancing act at hand and the potential economic costs that industry may bear. Concerns about cost are exacerbated given the gloomy economic outlook for Australia, now in its first recession since the early 1990s, and amid ongoing global market volatility.

Further to *Australia's Cyber Security Strategy 2020*, the CSCRC notes costs can be mitigated by approaching risk and security as a *shared responsibility*, with the Federal Government signalling its intent to assist critical infrastructure entities, when needed. The Strategy notes how success in strengthening the nation's cyber security posture rests on taking a **multi-stakeholder** approach to building cyber security resilience across the economy. Collaboration and the creation of a 'cyber security community' is the core of the strategy. Furthermore, the strategy places great focus on bolstering cyber security for small-to-medium-sized enterprise (SMEs), through the provision of

[3] https://www.homeaffairs.gov.au/cyber-security-subsite/files/2020-cyber-security-strategy-iap-report.pdf, pp. 9

various packages and initiatives. This includes leveraging the capabilities of large enterprise to secure Australian SMEs with tailored, cost-effective packages designed to increase the cyber security posture of small business. This approach was foreshadowed in the *Industry Advisory Panel Report*, which clearly championed the need for businesses to shoulder the cyber security burden together, highlighting the need for shared accountability to ensure the future digital sovereignty of Australia. Further, we acknowledge this is a matter for Federal Government to consider particularly in the context of financial constraints for all businesses in light of COVID-19.

We are living through a period of great upheaval. Amid a global pandemic unfolding against the backdrop of heightened geopolitical tensions, we must navigate an increasingly interconnected future, one driven by burgeoning 5G networks and billions of IoT devices. The centrality of digital connectivity in Australians' lives, and with the rest of the world, is certain. There is a clear opportunity for Australia to chart a new course – securing the essential services all Australians rely on and establishing a clear and more secure way forward for our digital future.