CYBER SECURITY
COOPERATIVE
RESEARCH
CENTRE

SUBMISSION:

Review of the Security Legislation Amendment (Critical Infrastructure) Bill 2020 and Statutory Review of the Security of Critical Infrastructure Act 2018

cybersecuritycrc.org.au

Dear Sir/Madam,

Submission: *Review of the Security Legislation Amendment (Critical Infrastructure) Bill 2020 and Statutory Review of the Security of Critical Infrastructure Act 2018*

I am pleased to submit the Cyber Security Cooperative Research Centre's (CSCRC) response to the Parliamentary Joint Committee on Intelligence and Security regarding its *Review of the Security Legislation Amendment (Critical Infrastructure) Bill 2020 and Statutory Review of the Security of Critical Infrastructure Act 2018*.

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 any future consultation regarding this very important topic.

Yours Sincerely,

Rachael Falk
CEO, Cyber Security Cooperative Research Centre
ceo@cybersecuritycrc.org.au

Introduction

The Cyber Security Cooperative Research Centre (CSCRC) welcomes the opportunity to provide this submission to the Parliamentary Joint Committee on Intelligence and Security regarding the *Review of the Security Legislation Amendment (Critical Infrastructure) Bill 2020 and Statutory Review of the Security of Critical Infrastructure Act 2018*. This submission follows our September 2020 submission concerning the Department's *Protecting Critical Infrastructure and Systems of National Significance* consultation paper and our November 2020 submission – *Security Legislation Amendment (Critical Infrastructure) Bill 2020 – Exposure Draft and Explanatory Document*.

The CSCRC broadly supports the efforts of the Australian government to bolster the resiliency and security of our critical infrastructure and systems of national significance, which provide essential services across the day-to-day lives of all Australian citizens. As per the statutory review of the *Security of Critical Infrastructure Act 2018* in conjunction with the Bill review, the CSCRC would like to provide feedback on the operation, effectiveness and implications of the Act by considering the appropriateness of having a unified scheme that covers all infrastructure assets (including telecommunication assets) that are critical to: (i) the social or economic stability of Australia or its people; or (ii) the defence of Australia; or (iii) national security.

Operation

The CSCRC commends the Federal Government for the expanded definition of Australian critical infrastructure to 11 sectors. The broadened approach and inclusion of additional sectors now more adequately captures Australia's economy, helping to ensure the future economic well-being of our nation. This expansion could not be more timely, given ongoing and sustained cyber activity undertaken globally against essential services and critical infrastructure providers. On 9 February 2021, authorities in the Florida town of Oldsmar reported that hackers had attempted to poison the town water supply by hacking into a

water treatment facility through a widely used software program. While the crisis was quickly averted, the attack is a sobering reminder of the potentially catastrophic effects that can be wrought by cyber attacks on the wider population, through critical infrastructure providers, even at the municipal level. Significantly, under the proposed expanded definition, water and sewerage will now be encompassed.

Furthermore, the inclusion of the financial services sector, higher education and research, and healthcare and medical are particularly pertinent, given the heightened threat environment since the beginning of the COVID-19 pandemic directed towards these sectors. On the former, on 25 January 2021, the Australian Securities and Investments Commission (ASIC) revealed that it had been hacked in a cyber attack which impacted approximately 130 entities who were applying for an Australian credit license.

Australia's higher education and research sector is also directly in the line of sight of nefarious cyber actors. The Australian Security Intelligence Organisation (ASIO), in its submission to a joint parliamentary inquiry into current risks faced by the Australian university sector, highlighted that Australia's research institutions remain vulnerable to exploitation, infiltration and data exfiltration through cyber means, outlining their awareness of "attempts to steal sensitive Australian intellectual property as part of cyber compromises". And the healthcare sector globally has been under siege since the beginning of the COVID-19 pandemic. At the close of 2020, Europe's top drug regulator, the European Medicines Agency, revealed it had suffered a cyber attack whereby confidential data about Pfizer Inc. and BionNTech SE's COVID-19 vaccine had been accessed, later found circulating on the dark web. This incident was preceded in September of 2020 when Düsseldorf University Hospital suffered a ransomware attack that severely disrupted emergency care and allegedly contributed to a 78-year-old patient's death, after cyber criminals reportedly exploited a known network vulnerability. Although prosecutors later failed to find legal causation between the cyber attackers and direct cause of death, the fatality stands as a

warning that future deaths could indeed be directly tied to a cyber security attack. Elevated threat levels on healthcare critical infrastructure networks worldwide have become the norm in recent years. Australia is not immune: in 2019, several Victorian hospitals suffered network attacks. Fortunately, cyber responders were able to effectively quash the attacks, preventing a possible data breach. The incidents underscore the sobering and very tangible impacts cyber security attacks can have on citizens.

As to how to effectively operationalise this expansion, the CSCRC recommends a number of practical measures to achieve the enhanced reforms:

- First, the CSCRC contends that the proposed reinvigorations to the Trusted Information Sharing Network (TISN) and Critical Infrastructure Resilience Strategy will enhance communications, trust and sharing of threat intelligence about cyber and physical threats and build collective awareness across government and industry of best practice, thereby solidifying critical infrastructure owners and operators' knowledge of threat environments. To enhance cyber mitigation strategies and effectively strengthen the resiliency of Australia's critical infrastructure sector, any information sharing should also be undertaken in a timely fashion, with pertinent advice and information for relevant organisations. That is, government can practically support critical infrastructure organisations' awareness of the cyber security threat landscape through the provision of real-time threat and vulnerability sharing with relevant entities, ensuring they are sufficiently engaged and informed. This will not only facilitate more open communications between government and organisations but will enhance organisations' understanding of supply chain cyber security risks, both downstream and upstream.

- The government has already made a crucial distinction, which will assist in the operationalisation of the proposed changes. This is found in the characterisation of 'information technologies and communication networks' and 'physical facilities' on equal footing. This effectively renders online and offline activity of equal significance, elevating cyber security threats to critical infrastructure to the appropriate level. Given that almost all organisations now run their networks and communications on digital systems, which remain inherently vulnerable to malicious cyber activity, the CSCRC recommends that government continue to underscore to relevant entities the vital importance of the 'secure by design' principle. Lastly, communication by government with relevant stakeholders should be unified and harmonised, with the provision of clear guidance as to what kind of support will be provided, what it will entail and how organisations can access it.
- The CSCRC notes that the key element to operationalising forthcoming legislative changes is approaching risk and cyber security as a *shared responsibility*. This approach has been articulated in *Australia's Cyber Security Strategy 2020*, which outlines the Federal Government's intent to assist relevant critical infrastructure providers, as needed, throughout this period of change. The Strategy underscores that Australia's national cyber security posture will only be strengthened if a **multi-stakeholder** approach is deployed, one which leverages the expertise and resourcing found across respective government and industry partners. That is, collaboration remains a central, methodological element to achieving cyber security resilience across the economy. For example, the CSCRC has highlighted in this and previous submissions the appropriate role and responsibility of government to clearly convey the required and pertinent elements of forthcoming legislation to industry, among other things. We also note that industry has a central role to play in a nation-wide cyber security uplift. In relation to the January 2021 ASIC hack, the need for 'corporates' to shoulder the burden when preventing cyber risk has been noted: "it would be a breach of their directors' duties if directors are not considering cyber risk on a regular basis. It's not a one-off tick-a-box

approach".[1] Furthermore, the Strategy underscores the need for large enterprise to assist small-to-medium-sized enterprise (SMEs) through the provision of cost-effective packages that will bolster their cyber security. Given that SMEs are the backbone of Australia's economy, accounting for almost 98 per cent of businesses, yet remain financially and resource-constrained particularly as it comes to uplifting their cyber security posture, a more significant role for large enterprise will help grow their awareness and capability at scale and contribute to a nation-wide security uplift.

Effectiveness

The CSCRC contends that proposed changes will be most effective if they are harmonised with Australian and international standards, to prevent regulatory 'overload'. We note that the principles-based outcomes proposed for critical infrastructure and systems of national significance currently correlate well with the Australian Cyber Security Centre's (ACSC) *Essential Eight*. However, there are multiple domestic regulatory bodies, which, for boards of critical infrastructure entities, could cause confusion as to which regulation they are required to comply with. For example, the Australian Prudential Regulation Authority (APRA) currently regulates financial services critical infrastructure entities through CPS234 [Prudential Standard CPS 234 Information Security]. However, the Australian Energy Market Operator (AEMO) currently sets minimum standards and regulatory requirements for energy sector critical infrastructure providers. Therefore, ensuring changes are implemented harmoniously entails a number of considerations. First, it would be beneficial for Australian sector regulators to be provided with enhanced knowledge about current cyber security threats and risks to their entities. This could be provided through regular and ongoing briefings to sector regulators by relevant cyber security experts. Secondly, the provision of clear and implementable guidance to sector regulators will facilitate their awareness of the increased scope of their responsibilities. Lastly, for organisations, clear

[1] Ishak, Robert, https://www.smh.com.au/business/banking-and-finance/corporate-watchdog-asic-hit-with-cyber-attack-20210126-p56wtr.html

communication about which regulator(s) they must comply with and what their cyber security obligations entail, will prevent confusion as to which operational standards to adopt.

The CSCRC also contends that efforts to achieve effectiveness will be hamstrung if consideration of international regulatory standards is not given. Considering that many of Australia's critical infrastructure providers maintain global operations with offshore subsidiaries, most notably in the financial services sector, relevant owners and operators must be provided with clear guidance as to international regulatory regimes and possible implications for their business.

In addition, effectiveness will only be achieved if regulatory changes are implemented through a phased transition period, in the vein of the approach taken by the *General Data Protection Regulation* (GDPR) in Europe. Although GDPR was adopted by the European Union in 2016, its provisions were not compulsory by relevant Member States until May 2018. Such an approach is advisable on two fronts. First, given that the expanded definition of critical infrastructure providers and systems of national significance now encompasses 11 sectors (previously four), consideration should be given to varying degrees of cyber maturity and readiness across those sectors, some which will require more significant uplift than others. Second, all relevant critical infrastructure entities will need adequate time to take preparatory measures to ensure compliance with forthcoming regulation. Accordingly, a sufficient 'grace' period should be designated for all sectors to prepare for compliance to ensure that there are no 'gaps', given that additional resources and processes may be required by entities to effectively adapt.

The CSCRC notes the importance of collaboration in achieving effectiveness. That is, many of the Bill's proposed reforms – including an enhanced TISN and Positive Security Obligation rules – are to be co-designed between government and industry. Certainly, a more pronounced role for industry in shaping the proposed reforms will ensure ongoing responsivity from the business community given the widespread appetite for reform(s) and bolstered security measures pertaining to critical infrastructure.

In addition, any regulatory frameworks and requirements enacted through the Bill must undergo regular review to ensure their robustness and relevance, given the fast-moving pace of onshore and offshore cyber threats. In Australia and other nations, the failure of regulation to keep up with digital, amorphous threats has tended to result in legislative 'lag', whereby measures quickly become obsolete and ineffective at responding to ever-evolving threats. This proposed approach is prudent and sensible, especially given the varying levels of cyber maturity found across Australia's critical infrastructure providers.

Lastly, effectiveness in managing cyber security risks for critical infrastructure providers will best be achieved through the following mechanisms: timely and relevant information about current cyber security threats; defined recommendations and guidelines as to how to achieve cyber security uplift; and a continuous and demonstrated effort to share threat intelligence and maintain transparency concerning threats to Australia's national security and sovereignty. A further, critical element is urged, in recognition of the required technical expertise and resourcing required by entities to achieve cyber 'inoculation'. That is the possibility of practical, hands-on assistance from relevant cyber security experts to critical infrastructure entities as to 'how' to implement the required guidelines and obligations, if needed, given different degrees of cyber maturity found across newly encompassed sectors. An example of this type of assistance was the November 2019 national cyber security exercise series, hosted by the Australian Cyber Security Centre in collaboration with a select group from across Australia's electricity industry and government agencies,

both at the federal and state level. Designed specifically with potential cyber incidents in mind, similar preparatory events should be considered and potentially offered to all critical infrastructure providers in the future on a regular basis.

Implications of the Act

The CSCRC notes that the security uplift required to fulfil obligations in the Bill will entail legislative imposts for industry, given proposed penalties for non-compliant business. Mitigating the potential for foreign or cyber interference in Australia's most critical services while protecting the sovereignty and economic and national security of our nation is, indeed, a delicate balancing act. In consideration of this, the CSCRC recommends that various incentivisation schemes might be tabled for relevant entities to lessen the burden on business. These mechanisms might include instant asset write offs and tax breaks, which would not only ease the impost on business but also simultaneously increase the resilience of Australia's critical infrastructure and systems of national significance.

In addition, a harmonised (both global and domestic) and interoperable Act will prevent regulatory confusion, helping to ensure that critical infrastructure providers respond to the relevant regulator, not multiple regulators. This will have a secondary effect of ensuring that legitimate and concrete cyber security resilience is achieved rather than mere compliance and regulatory overload. Furthermore, from a global perspective, it will also ensure that Australian critical infrastructure providers are not hampered in their overseas operations, given the global, digital and dispersed nature of their businesses.

Lastly, the CSCRC would like to highlight that the Federal Government's efforts to create positive security obligations for critical infrastructure providers is, by and large, a positive and proactive move, one which will have significant and long-lasting effects for our nation, our national security, and all Australian citizens. These obligations draw a significant line in the sand, signalling to the Pacific region and the rest of the world Australia's forward-thinking and holistic approach to mitigating cyber security threats. To the international community it demonstrates Australia's leading commitment to global best practice in cyber security, through the setting of an example for our neighbours and allies to follow, potentially triggering a cyber uplift 'domino effect' across the region. If a significant uplift were to occur across the Pacific region, Australia would cement its position as a safe and trusted place to do business and as a nation committed to ensuring the stability and security of all citizens.