CYBER SECURITY
COOPERATIVE
RESEARCH
CENTRE

SUBMISSION:

Security Legislation Amendment (Critical Infrastructure) Bill 2020 – Exposure Draft and Explanatory Document

cybersecuritycrc.org.au

Dear Sir/Madam,

Submission: *Security Legislation Amendment (Critical Infrastructure) Bill 2020* – Exposure Draft and Explanatory Document

I am pleased to submit the Cyber Security Cooperative Research Centre's (CSCRC) response to the Department of Home Affairs regarding its *Security Legislation Amendment (Critical Infrastructure) Bill 2020* (the Bill) – Exposure Draft and Explanatory Document. We commend the Federal Government for its commitment to ensuring Australia remains a secure nation and trusted place to do business through enhanced measures to bolster systems and infrastructures essential to the daily lives of all 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 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 Department of Home Affairs regarding the *Security Legislation Amendment (Critical Infrastructure) Bill 2020* (the Bill) – Exposure Draft and Explanatory Document. This follows our September 2020 submission concerning the Department's *Protecting Critical Infrastructure and Systems of National Significance* consultation paper. Then, as now, the CSCRC notes the timeliness of developments in this space, given rapidly evolving cyber threat vectors and the pressing need to secure Australia's increasingly networked critical infrastructure.

The heightened cyber threat environment globally stands as a stark reminder of the need for robust legislative and regulatory safeguards for critical infrastructure and systems of national significance. Verizon's recently released *Cyber Espionage Report* [1] highlights that from 2014-2020, the sectors most frequently targeted by malicious cyber actors and subject to cyber espionage breaches globally include: education, financial services, information, manufacturing, mining and utilities and professional services and the public sector. It is notable a number of these sectors have now been captured within the Bill, with its expanded and broader definition of eleven critical sectors. The CSCRC notes the broader definition now captures a much larger segment of the economy across both the public and private sectors and contends that this is essential given the pivotal role played by critical infrastructure in delivering essential services to all Australians.

The Bill expands on Australia's progressive stance in protecting critical infrastructure and our most valuable and essential assets, leveraging the existing protections in the *Security of Critical Infrastructure Act 2018* with enhanced regulatory considerations to help ensure the future safety of Australia's citizens and systems of critical importance. Significantly, the

[1] https://enterprise.verizon.com/resources/reports/2020-2021-cyber-espionage-report.pdf, p. 4

Bill's mechanisms, if adopted, will ensure Australia will be a leader in global best practice. For example, the European Union (EU), the global standard-bearer concerning data and privacy sharing as a result of its General Data Protection Regulation (GDPR), until very recently continued to operate under the *2008 Directive on European Critical Infrastructures* (Council Directive 2008/114/EC).[2] The Directive presented a European-wide approach to the designation of critical infrastructure and a shared understanding for ensuring their protections. Critically, the Directive was only applicable to energy and transport sectors. On 24 June 2020, following a 2019 external evaluation,[3] the Directive was updated to reflect the digital challenges faced by a broad range of critical infrastructure. It is notable that it now includes "any system which is essential for providing vital economic and social functions",[4] which, like Australia's Bill, comprises health, food, security, information systems and financial services, along with others. Such a position is holistic and forward facing, and will help mitigate potential security threats and bolster the resilience of critical infrastructure across a wide breadth of the economy. The CSCRC notes the Bill builds on the EU Directive and goes much further in mandating the protection of critical infrastructure and systems of national significance.

Cyber security as a threat vector

The Bill's sharpened focus on mitigating cyber security threats is important, with the CSCRC noting the recognition of these 'intangible' threats in equal billing with more traditional, physical threats, is the correct direction for government to take. This has a two-pronged and positive effect. First, it comes alongside a more pronounced role for the Australian Signals Directorate (ASD) through the Australian Cyber Security Centre (ACSC), the organisation vested with the responsible oversight of our nation's cyber security posture.

[2] https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF
[3] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/1631-Evaluation-of-the-2008-European-Critical-Infrastructure-Protection-Directive
[4] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12462-Enhancement-of-European-policy-on-critical-infrastructure-protection

Under the proposed Positive Security Obligation for critical infrastructure providers, organisations will now be required to report serious cyber security incidents to the ACSC. Given the ASD recently received an augmentation of its offensive cyber security capabilities,[5] to reinforce its efforts to 'actively disrupt' overseas malicious cyber activity and protect Australia's interests, the CSCRC contends this will strengthen the Federal Government's national cyber threat assessment capabilities, leading to more holistic, whole-of-nation approaches to mitigating serious cyber and national security risks. Secondly, the new requirements in the Bill for critical infrastructure to "develop and comply with a critical infrastructure risk management program" (p 43, Explanatory Doc) as part of the forthcoming Positive Security Obligation, will require entities to critically address "cyber security risks" alongside physical, personnel and supply chain risks (p 47, Explanatory Doc). The elevation of cyber security threats alongside other well-known risks will ensure entities' responsivity to an ever-changing threat environment, given their systemic reliance on digital systems – the ubiquitous communications backbone on which their networks run. The globally interconnected nature of these communication networks remains, at all times, vulnerable to cyber security threats.

The importance of co-design

The CSCRC notes that many of the Bill's proposed reforms – including an enhanced Trusted Information Sharing Network (TISN) and Positive Security Obligation rules – are to be co-designed between government and industry. This perspective aligns with *Australia's Cyber Security Strategy 2020*, which advocates for a multi-stakeholder approach to building cyber security resilience across the economy, promoting cyber security as a ***shared responsibility***. Eschewing a top-down, government-led approach, the proposed reforms in the Bill advocate for sustained collective action and procedures by government, business and regulatory bodies to integrate a more effective and economy-wide cyber security uplift

[5] https://www.abc.net.au/news/2020-06-29/cyber-security-investment-link-attacks-scott-morrison/12404468

across the Australian economy. Certainly, a more pronounced role for industry in Australia's cyber security ecosystem will ensure ongoing responsivity from the business community given the widespread appetite for reform(s) and bolstered security measures pertaining to critical infrastructure.

Recommendations:

The CSCRC has several key recommendations that will help ensure that, if enacted, the Bill is effective in practice.

1. Phased implementation

The CSCRC recommends a phased implementation approach,[6] modelled after the EU's GDPR model, to ease onerous legislative imposts upon business and facilitate a smoother implementation period. That is, a transition period is advisable, one whereby relevant critical infrastructure entities will be able to take adequate preparatory measures to ensure compliance with forthcoming regulation. This phased approach should be clearly articulated to all critical infrastructure providers, establishing a clear framework within which business can effectively operate with certainty. This recommendation is prudent, considering varying levels of security awareness and understanding across sectors which will be newly captured by the Bill, which previously may have had lower levels of cyber maturity than already-designated critical infrastructure providers and which may require significant uplift. There should be an allocated 'grace' period for these sectors to adapt to new requirements, allocate resources appropriately across their organisations and also ensure that from a people and processes perspective, they are adequately prepared to participate in an ecosystem-wide security uplift. On the latter point, *Australia's Cyber Security Strategy 2020*[7] highlights the national critical skills shortage of cyber security professionals. Hence, there is a pressing need to build a pipeline of cyber security talent.

[6] https://www.infosecurityeurope.com/en-gb.html?v=636289786574700000
[7] https://www.homeaffairs.gov.au/about-us/our-portfolios/cyber-security/strategy

Considering this skills gap, government and industry action in this capacity should be immediate and active, with a focus on implementing agreed accreditation standards for Australian cyber security professionals.

2. Requirement for regular review

The CSCRC recommends that, if enacted, the mechanisms and regulatory frameworks underpinning the Bill be regularly reviewed to ensure they remain fit-for-purpose. An ongoing and consistent review process would help mitigate the risk that the Bill's measures quickly become obsolete or ineffective at responding to newly established cyber security threats, ensuring that regulatory mechanisms are robust, up-to-date and responsive. Such an approach would ensure the provisions continue to be relevant and suitable for the digital age. As seen in Australia and other nations, regulation has often failed to keep pace with technological advancements and advanced cyber threat techniques. Exemplifying the escalating cyber threat environment globally, offshore cyber crime syndicates are diversifying criminal cyber activity, moving to a more sophisticated 'franchise' model[8] to deploy malware and achieve scalability. Increasingly available via the dark web, the new model creates a malware supply chain, whereby cyber criminals 'rent' viruses and ransomware to distributors, effectively making cyber attacks much more difficult to attribute. This disturbing new trend was also highlighted by Microsoft's annual *Digital Defense Report*[9] which noted the rapidly evolving sophistication of nefarious cyber actors and their adept appropriation of new techniques. Considering the fast-moving pace of technological advancement and rapidly evolving security threats, and given that newly captured critical infrastructure providers currently have varying levels of cyber maturity, the proposed approach is sensible.

[8] https://www.afr.com/politics/federal/cyber-criminals-renting-out-their-malware-expert-warns-20201012-p5648g
[9] https://www.microsoft.com/en-us/download/details.aspx?id=101738

3. Incentivisation measures

The CSCRC submits the security uplift required to fulfil obligations detailed in the Bill will come at a cost. Furthermore, the exposure draft outlines proposed penalties for business, should they fail to comply with forthcoming obligations. Considering this and to lessen the burden on business, the CSCRC submits that various incentivisation schemes should be considered for critical infrastructure providers that can demonstrate their compliance and adherence to regulatory requirements. Such measures could include tax breaks and instant asset write offs, which would have a two-pronged effect and make economic sense, simultaneously easing the impost on industry while also hardening critical infrastructure and systems of national significance.

4. Real-time threat and vulnerability sharing

The CSCRC urges government to conduct real-time threat and vulnerability sharing with industry partners, to effectively assist critical infrastructure entities, particularly those newly captured organisations, to understand and manage risks. Further to the CSCRC's earlier recommendation[10] that an improved Trusted Information Sharing Network (TISN) should include mechanisms to bolster communications, trust and sharing of threat intelligence about physical and cyber threats, we are encouraged to see the proposed enhanced mechanisms in the Bill to strengthen the functionality and effectiveness of the TISN. Furthermore, the multi-stakeholder approach to this endeavour proposed in the Exposure Draft, whereby the enhanced TISN will be co-designed together with industry, ensures that the mechanism will remain industry-driven and that uptake across business will likely increase. The demonstrated approach to the revised TISN will ensure that maximum impact is achieved, and that information is shared in a timely manner with useful

[10] https://www.homeaffairs.gov.au/reports-and-pubs/files/critical-infrastructure-consultation-submissions/Submission-112-Cyber-Security-Cooperative-Research-Centre.PDF

insights for relevant critical infrastructure stakeholders and government agencies, thereby hardening Australia's critical infrastructure.

5. Harmonisation

Careful consideration needs to be given as to interoperability and harmonisation of proposed regulatory obligations and requirements to avoid a 'battle of the laws' which in the event of a serious breach could result in a critical infrastructure provider responding to multiple regulators. This will also help ensure that tangible cyber security uplift is achieved as opposed to compliance overload. This will not only ensure that critical infrastructure providers themselves do not suffer from regulatory confusion and overload but also from a global perspective, that Australia's critical infrastructure providers are not impeded in the delivery of the day-to-day essential services Australians rely on, given the globally interconnected nature of their businesses and the cross-border dependencies inherent in existing supply chains.

6. Greater clarity regarding the Government Assistance regime

The CSCRC submits that greater clarity is needed regarding the proposed Government Assistance regime. These powers, what they mean, how they will be used and by whom needs to be clearly articulated. This will involve close consultation with industry and other stakeholders to ensure the regime is both clearly understood and proportionate. While more work is needed, the CSCRC is encouraged to see appropriate checks and balances built into the Bill regarding the regime. These changes propose that government, when it is deemed essential and of utmost necessity, will maintain "ultimate responsibility for protecting Australia's national interests. As a last resort, the Bill provides for Government assistance to protect assets during or following a significant cyber attack" (p 7, Explanatory Doc). The CSCRC notes the oversight mechanisms for obtaining approval for assistance by the Department of Home Affairs outlined in the Exposure Draft are robust, proportionate

and appropriate to ease the concerns of business that the Bill offers too much leeway to the Federal Government to intervene[11] in response to security incidents.

Conclusion

In conclusion, the CSCRC is broadly supportive of the Federal Government's efforts to uplift Australia's critical infrastructure through the Bill's proposed changes. The effects will be consequential for our nation and our national security, with significant flow-on effects for all Australian organisations and residents. The proposed legislation will provide clarity for organisations captured under the revised measures and will generate an economy-wide security uplift which, globally, is setting an example for our allies and neighbours. Such efforts also reinforce that cyber security must remain a foremost consideration for government and businesses in today's digital economy, one whereby cyber security threats remain an ever-present concern.

[11] https://www.innovationaus.com/concern-over-rushed-critical-infrastructure-law/?utm_medium=email&utm_campaign=Newsletter%20442%20-%2012%20November%202020&utm_content=Newsletter%20442%20-%2012%20November%202020+CID_f6240d26ed34c092030955b10f1b1377&utm_source=Email%20marketing%20software&utm_term=Concern%20over%20rushed%20critical%20infrastructure%20law