CYBER SECURITY
COOPERATIVE
RESEARCH
CENTRE

CSCRC SUBMISSION: Response to the Department of Home Affairs – *Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022 – Exposure Draft and Explanatory Document*

cybersecuritycrc.org.au

Dear Sir/Madam,

Submission: *Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022* – 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 Protection) Bill 2022* (the Bill) – Exposure Draft and Explanatory Document. Enhanced legislative provisions to uplift the cyber security of Australia's critical infrastructure and systems of national significance are essential to ensuring Australia's ongoing prosperity and national security. Hence, the CSCRC is supportive of action being taken by the Federal Government to bolster the security of essential services and systems via the *Security Legislation Amendment (Critical Infrastructure) Act 2021*, which will be further enhanced by the Bill.

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.

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 (the Department) regarding the *Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022* (the Bill) – Exposure Draft and Explanatory Document. This follows our ongoing engagement with the Department in relation to legislative enhancements aimed at protecting Australia's critical infrastructure and systems of national significance, which has so far seen the passage of the *Security Legislation Amendment (Critical Infrastructure) Act 2021* (SLACI Act).

The CSCRC would like to note the highly consultative and collegiate nature of the process thus far. This has seen the Department work closely with industry and key stakeholders to help ensure these significant legislative changes are effective, fit for purpose and mitigate the risk of unintended consequences.

The Bill at hand reflects the suggested changes and enhancements to the SLACI Act in line with recommendations made by the Parliamentary Joint Committee on Intelligence and Security's (PJCIS) advisory report into the *Security Legislation Amendment (Critical Infrastructure) Bill 2020*. It also illustrates further consultation has been undertaken with sectors specifically impacted to help ensure changes are not unduly burdensome and, most importantly, are achievable.

Given the CSCRC's significant engagement to date, this submission takes a high-level approach to the Bill and its provisions. Strengthening the cyber security of Australia's critical infrastructure and systems of national significance is vital to ensuring the safety and security of Australians and maintaining Australia's reputation as a safe and trusted digital economy. Hence, the CSCRC is supportive of the Federal Government's moves to mandate cyber bolstered cyber security requirements for captured sectors. Ultimately, this will have a knock-on effect of enhancing cyber security more broadly across vital supply chains and the wider economy.

Establish, maintain, and comply with a Risk Management Program

Risk Management Programs

The establishment of Risk Management Programs (RMPs) for particular entities would help enhance the overall effectiveness of changes to critical infrastructure legislation. It is encouraging that clear steps have been taken within this section of the Bill to help prevent duplication of existing obligations, which would be onerous and burdensome on impacted entities.[1] And where strong frameworks are already in place, the Bill helps ensure these would not be weakened by the introduction of new, less stringent cyber security baselines.

RPMs themselves will be important in helping establish an overall picture of the cyber security (and more general security) posture of captured entities. As it stands, there is little insight into the cyber posture of many of Australia's critical infrastructure entities, with a more holistic understanding assisting in the development of targeted interventions and assistance in areas where posture could be improved. As noted in the EM, "the RPM itself would provide a tool for Government to verify whether the risk mitigation approach taken by the responsible entity is appropriate in protecting Australians' access to essential services". Furthermore, it would also serve to allow captured entities themselves have a thorough understanding of their own cyber posture and gaps. It is vital that any RPM be an effective program and does not become seen as just a compliance-related activity. The CSCRC is supportive of the introduction of fines for non-compliance. While such an approach represents a stick rather than a carrot, fines would incentivise affected entities to comply with the proposed obligations and is an appropriate mechanism to help ensure compliance.[2]

While the proposed legislation states programs should be reviewed on a 'regular basis', no definition of what this means is provided, though justification for this wording is provided in the EM. The CSCRC submits greater clarity as to what constitutes a 'regular basis' is required to help ensure adequate cyber security is maintained across the economy. Hence, the CSCRC recommends a mandated annual view be considered. This would align with the proposed requirement for annual reporting to the Secretary of Home Affairs[3] and, in the CSCRC's view, would not be overly burdensome.

[1] Explanatory Document (homeaffairs.gov.au), P5
[2] Explanatory Document (homeaffairs.gov.au), P12
[3] Explanatory Document (homeaffairs.gov.au), P15

Positive Security Obligations

The CSCRC supports the creation of Positive Security Obligations (PSOs) for particular critical infrastructure assets at the discretion of the Minister for Home Affairs.

As noted in the EM, "the regime would embed preparation, prevention and mitigation activities into the business-as-usual operation of critical infrastructure assets, providing certainty for businesses across all critical infrastructure sectors by setting clear security standards".[4] Such an approach is prudent in the current environment, where threat vectors continue to increase and grow in sophistication, with critical infrastructures a key target of such nefarious activity.

The inclusion of a six-month transition to PSO commencement (as a minimum) would provide affected entities with adequate time to comply and make reduce the burden for business.[5]

Enhanced Cyber Security Obligations for Systems of National Significance

Systems of National Significance

The establishment of Systems of National Significance (SoNS) is necessary and would help ensure Australia's most acutely critical infrastructure is identified and has heightened security against cyber and physical threats. As noted in the EM, "SoNS are proposed to be a significantly smaller subset of critical infrastructure assets that, by virtue of their interdependencies across sectors and cascading consequences of disruption to other critical infrastructure assets and critical infrastructure sectors, are crucial to the nation". [6] It is important the Minister for Home Affairs be granted discretionary and targeted powers with a "stated security objective" to privately declare a critical infrastructure asset a SoNS, taking into account an asset's interactions and interdependencies with other critical infrastructure assets, as well as the potential impacts of a serious attack on such assets for the wellbeing of the nation more generally.[7] Such an approach would also help impacted entities identify and target cyber uplift spending into specific areas where bolstering cyber security is most important.

Enhanced Cyber Security Obligations

Developing an information sharing culture will be essential to ensuring the success of changes to Australia's critical infrastructure legislation. Central to this is strong relationships between critical infrastructure entities and government, which would be supported by

[4] Explanatory Document (homeaffairs.gov.au), P10
[5] Explanatory Document (homeaffairs.gov.au), P11
[6] Explanatory Document (homeaffairs.gov.au), P6
[7] Explanatory Document (homeaffairs.gov.au), P6

Enhanced Cyber Security Obligations (ECSOs) for SoNS. As noted in the EM, such obligations "would support the bi-directional sharing of threat information to provide industry with a more mature understanding of emerging cyber security threats, and the capability to reduce the risks of a significant cyber attack against Australia's most critical assets".[8]

The four elements of ECSOs that SoNS may be required to comply with under the Bill include:

- statutory incident response planning to ensure processes and tools are in place to prepare for and respond to cyber security incidents[9]
- participation in a cyber security exercise to test response preparedness, mitigation and response capabilities as required[10]
- vulnerability assessments to identify vulnerabilities in systems which expose them to particular types of cyber incidents[11]
- provision of system information to build a near-real time threat picture and share actionable, anonymised information back out to industry[12]

The CSCRC is supportive of the introduction of fines for non-compliance. The risk of fines would incentivise affected entities to comply with the proposed obligations and is an appropriate mechanism to help ensure compliance. However, in this regard we respectfully submit that enacting of fines be viewed as an option of last resort.

[8] Explanatory Document (homeaffairs.gov.au), P6
[9] Explanatory Document (homeaffairs.gov.au), P17
[10] Explanatory Document (homeaffairs.gov.au), P17
[11] Explanatory Document (homeaffairs.gov.au), P18
[12] Explanatory Document (homeaffairs.gov.au), P19