CYBER SECURITY
COOPERATIVE
RESEARCH
CENTRE

CSCRC SUBMISSION: PJCIS review of the Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022

cybersecuritycrc.org.au

Dear Sir/Madam,

Submission: PJCIS review of the *Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022*

I am pleased to submit the Cyber Security Cooperative Research Centre's (CSCRC) response to the Parliamentary Joint Committee on Intelligence and Security's (PJCIS) review of the *Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022* (the Bill). 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

Did you provide feedback on the exposure draft and do you feel like consultation was inclusive and wide-ranging?

The Cyber Security Cooperative Research Centre (CSCRC) did provide a submission to the Department of Home Affairs in relation to the exposure draft of the *Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022* (the Bill) – Exposure Draft and Explanatory Document. This followed 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).

In the submission, the CSCRC noted the highly consultative and collegiate nature of the process that has been undertaken in relation to changes to critical infrastructure legislation. 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.

Has your feedback been incorporated in the Bill or addressed in explanatory material?

The CSCRC did not propose any material changes to the Bill and felt it resolved issues raised during the wide-ranging consultation of the *Security Legislation Amendment (Critical Infrastructure) Bill 2020*. Specifically, the Bill reflects the recommendations made by the Parliamentary Joint Committee on Intelligence and Security's (PJCIS) report into the *Security Legislation Amendment (Critical Infrastructure) Bill 2020*, incorporating these recommendations into the new framework.

What are your five key themes of feedback on the Bill?

- The CSCRC is supportive of the Federal Government's moves to mandate cyber bolstered cyber security requirements for captured sectors.
- 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.
- 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.

- The CSCRC supports the creation of Positive Security Obligations (PSOs) for particular critical infrastructure assets at the discretion of the Minister for Home Affairs.
- 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 Enhanced Cyber Security Obligations (ECSOs) for systems of national significance.

Do you think the potential regulatory impact has been captured accurately?

The CSCRC submits that the regulatory impact has been captured accurately and clear steps have been incorporated into the Bill to avoid regulatory duplication. While the regulatory impacts of the Bill would be brought to bear if it passed, phasing-in measures as well as other mechanisms to reduce regulatory burden would reduce the risk of unintended consequences in this regard.

On balance, do you support the Bill in its presented form, recognising the risks facing critical infrastructure assets in Australia?

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.