

---

*Active Cyber Defence Alliance*

*Opening Statement for Public Hearing 8th July 2021*

*Parliamentary Joint Committee for Intelligence and Security*

---

ACDA Submission to PJCIS – Opening Statement for Public Hearing 8th July 2021

© Active Cyber Defence Alliance 2021



## Copyright Notice

This work is licensed under a Creative Commons Attribution 4.0 International licence (CC BY 4.0) (<http://creativecommons.org/licenses/by/4.0/deed.en>).

## Third Party Copyright

Wherever a third party holds copyright in this material, the copyright remains with that party. Their permission may be required to use the material. Please contact them directly.

## Attribution

This publication should be attributed as follows: *"ACDA Submission to PJCIS – Opening Statement for Public Hearing 8th July 2021"* and you must provide a link to the license. You may reproduce any material from this document but not in any way that suggests the licensor endorses you or your use.

## Disclaimer

The statements in this submission are the opinions of the authors as members of the Active Cyber Defence Alliance and do not necessarily reflect the views of their individual employers

### Opening Statement

In reviewing the Security Legislation Amendment (Critical Infrastructure) Bill 2020 (**the Bill**), the Active Cyber Defence Alliance (**ACDA**) has provided seventeen recommendations that we believe will drive better cyber security, better preparedness for a cyber security incident, greater clarity around cyber security issues for operators, and cyber security leadership for the Australian business community.

The legislation needs to include reportable management of information security linked to the risk-based approach already in the legislation. This will drive better cyber security for operators and regulators and remove an arbitrarily low baseline defined by the specific requirement of a handful of security controls.

Recommendations for sharing information and threat intelligence, clear lines of accountability, response exercises and active defence measures will all contribute to operators and regulators being better prepared for cyber security incidents.

The recommendations around the legality of interaction with the attackers in the event of a cyber security breach will provide greater clarity for operators and the regulators, as will the mandate for reportable management of information security.

If there is successful implementation of better cyber security practices across the critical infrastructure ecosystem based on a robust and progressive Security of Critical Infrastructure Act, then the benchmark will be set for other parts of the Australian economy to follow suit in implementing strong cyber security measures.

The ACDA has a particular focus on cyber security and providing recommendations for the defence of Australia through the security practices of all organisations. Thank-you for the opportunity to participate in this public hearing today.