Friday 29th August

Submission to the Australian Cyber Security Strategy – Horizon 2 Policy Discussion Paper

Submitted by [redacted], CS4CI | Author, Securing Society | CISM | ISA/IEC 62443 | SANS ICS418

Introductory Remarks

Firstly, I commend the Australian Government for the momentum achieved under Horizon 1. Elevating national cyber resilience is no small feat. The Horizon 2 consultation presents a crucial opportunity to close systemic gaps - especially around cyber-physical risk, the security of operational technologies (OT), and emerging edge environments like consumer energy resources (CER).

As a co-founder of the Cyber Security for Critical Infrastructure (CS4CI) community, our work brings together frontline operators, engineers, and cyber professionals to collaboratively strengthen cyber-physical safety. My white paper, *Securing Society: Insights on Cyber-Physical Safety in Australia's Critical Infrastructure*, was informed by this community and highlights urgent areas of concern. This submission reflects those insights alongside my 25 years technology and cybersecurity experience primarily in Critical Infrastructure (I've worked across 7 of the 11 SOCI Act sectors, both here in Australia and in the UK), supported by my industry cybersecurity certifications and courses; CISM, ISA/IEC 62443, and SANS ICS418.

3.2 Shield 2: Safe Technology

Q18 – International best practices for secure technology standards (edge, CER, OT)

Australia should look to international models that embed secure-by-design and secure-by-default principles not just in consumer IoT, but across the full device landscape - including commercial and industrial OT environments. Currently, the Cyber Security Act focuses narrowly on consumer-grade tech, leaving a regulatory gap in areas that interface with critical infrastructure.

Recommendations:

- Expand the Act's scope to cover commercial and OT devices, especially those deployed in critical sectors.
- Introduce minimum cyber-physical safety standards for edge-connected CER systems, aligned with international frameworks like AS IEC 62443, NIS2, and NIST SP 800-82.
- Mandate vendor disclosures of residual risk (e.g. default credentials, remote access exposure) in devices used in grid-edge and industrial settings.

- Incentivise cyber-physical vulnerability reporting and threat modelling practices during procurement of control and sensing equipment.

Through my research and community engagement, it's clear that **cyber-physical risk remains poorly understood** by many boards and operational leaders. There is a strong need for targeted guidance and board-level education to translate technical risks into governance priorities.

3.4 Shield 4: Protected Critical Infrastructure

Q34 – Risks not adequately addressed under the current framework

The most pressing gap is the absence of clear guidance for physical industrial control systems that are increasingly being exposed to cyber threats. Australia's current regulatory lens focuses heavily on information security, overlooking the operational impact of compromised control logic, unsafe actuator behaviour, or untrustworthy sensor inputs.

Further the SOCI Act and Cybersecurity Legislative Package focus on "digital" risk management, assuming that the mechanical functions of industrial control systems are inherently safe or covered by other safety standards. In today's connected, autonomous environments, this assumption creates a critical blind spot in our national cyber posture.

Primary Recommendation

Horizon 2 should extend secure-by-design and secure-by-default principles to physical and mechanical controls in critical infrastructure. Components like valves, actuators, and inverters must be treated as part of the attack surface, with guidance to ensure their secure engineering and operation.

Instances where control system components can be subject to cyberattacks to cause dangerous physical outcomes should be protected by these simple mechanical components by having them configured to provide a primitive but cyberattack-resistant line of defence against threats on associated control systems.

This is the most pressing of all our recommendations and is essential for true cyber-physical safety.

Other Recommendations:

- Incorporate control system-specific threat scenarios (e.g. unsafe state transitions, kinetic consequences) into the Critical Infrastructure Risk Management Program (CIRMP).

- Given the Australian Standard's adoption of AS IEC 62443 as the national standard, we recommend integrating this with the SOCI Act obligations for OT to align, provide consistency for industry and drive increased standardisation.
- Align existing frameworks with AS IEC 62443's Security Levels (SLs) to differentiate protection needs across sectors and system criticalities.
- Embed "safety consequence lenses" in cyber assessments - helping asset owners distinguish between confidentiality risks and mission failure risks.

Q36 – Proportionality of regulatory burden

Insights from *Securing Society* indicate that current regulations are still in their infancy when it comes to protecting society from cyber-physical disruption. Interviewees expressed that while the regulatory burden is growing, more needs to be done given the national importance of protecting against supplier failures of our essential services. Several also noted that many OT environments are still years behind in maturity and will require greater structured support.

Q36 – Support to uplift cyber and operational resilience

Critical infrastructure IS national security.

Our nations critical infrastructure cybersecurity resilience must evolve beyond the IT department. We must embed a **"whole-of-organisation" mindset** across engineering, operations, HR, and frontline staff roles (finance, reception teams, customer services etc).

Recommendations:

- Encourage organisations to build and leverage cross-disciplinary cyber-physical teams, bringing together IT, OT, industrial control process safety, engineers, safety practitioners and physical security professionals (security guards etc).
- Fund scenario-based cyber drills, modelled on physical fire drills, that simulate coordinated threat scenarios (e.g. ransomware + process upset) for whole of organisation response.
- Support development of a national cyber-physical security playbook, tailored to ICS/SCADA operators and based on international best practice (AS IEC 62443, NIS2, NIST 800-82).
- Enhance the upcoming Cyber Reservist Program to encourages general Critical Infrastructure staff (not just tech / cyber teams) to support national cyber incident response during crises and raise their own awareness in their organisations.
- Incentivise adoption of resilience engineering principles in control room environments, including consequence-based risk planning and system-of-systems thinking.

Final Comment

Australia's modern-day society, and the built environment that sustains it, is only as safe as the physical systems that control it. As our grid-edge expands, AI agents enter industrial environments, and critical infrastructure becomes increasingly autonomous, cyber-physical risk must become a national priority.

Through CS4CI and the Securing Society paper, I remain committed to helping government and industry bridge the gap between operational safety and cybersecurity, ensuring our infrastructure remains safe, resilient, and trustworthy.

This is not just a strategic necessity, it is our obligation to modern society, and a moral imperative we cannot ignore.

Finally, our community and myself are committed to improving our nations cyber-physical safety and welcome the opportunity to be further involved, please get in touch as appropriate.

Kind regards,

[redacted]

[redacted] CS4CI Community

CISM | ISA/IEC 62443 Cybersecurity Specialist | SANS ICS418

Cybersecurity Committee Member (Vic SIG) - Australian Computer Society (ACS)

Management Committee Member - Australian Control Room Network Association (ACRNA)