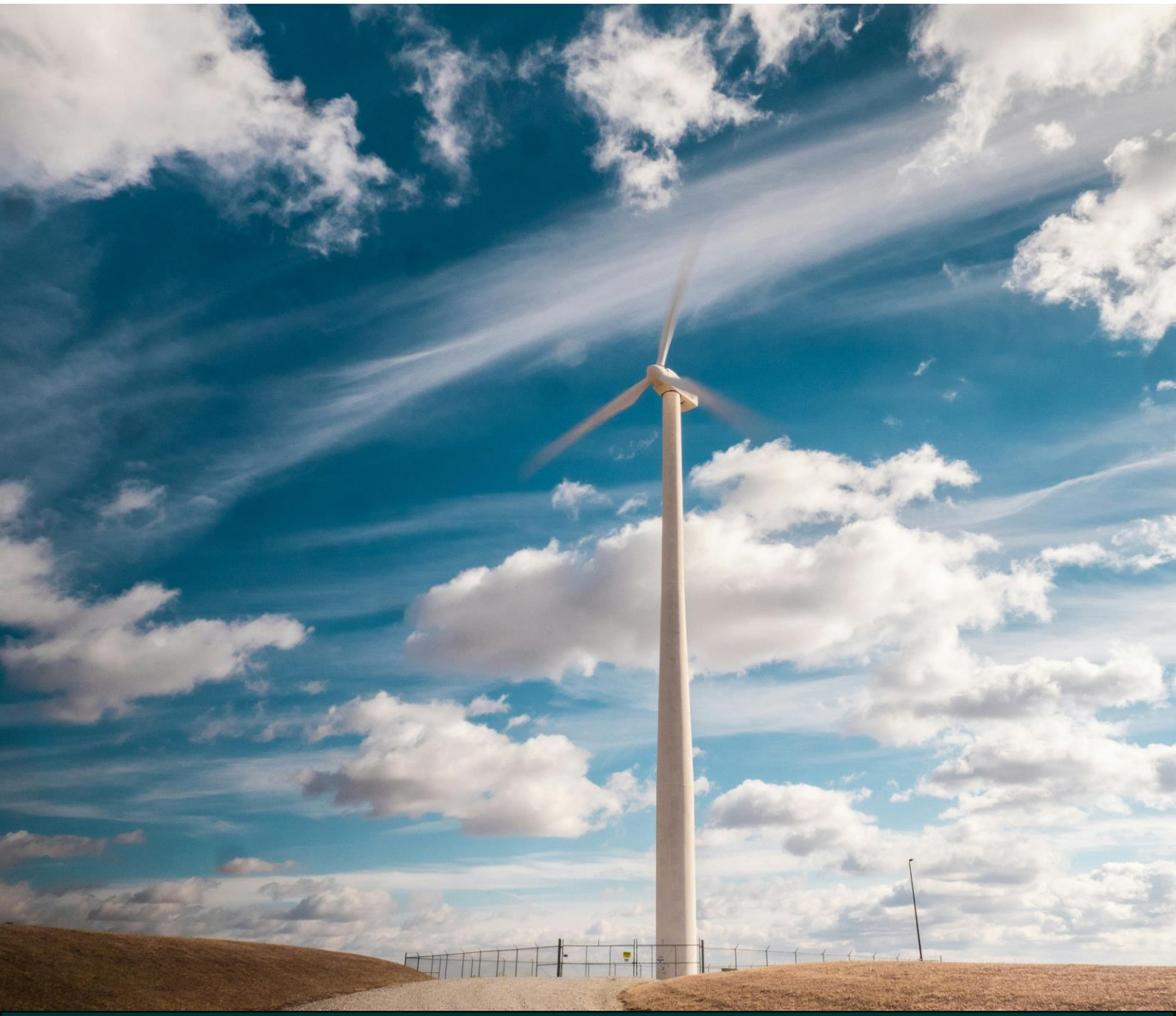


CLEAN ENERGY COUNCIL

Horizon 2 of the 2023-2030 Australian Cyber Security Strategy

Clean Energy Council Submission

Friday, 29 August 2025

Submitted online via Department of Home Affairs

Clean Energy Council Response to Horizon 2 of the 2023-2030 Australian Cyber Security Strategy Discussion Paper

The Clean Energy Council (CEC) welcomes the opportunity to provide feedback to the Department of Home Affair's (DHA) consultation on the Horizon 2 Discussion Paper of the 2023-2030 Australian Cyber Security Strategy.

The CEC is the peak body for the clean energy industry in Australia. We represent and work with Australia's leading renewable energy and energy storage businesses, as well as accredited designers and installers of solar and battery systems, to further the development of clean energy in Australia. We are committed to accelerating the transformation of Australia's energy system to one that is cleaner, equal, fair and transparent for all consumers.

We are supportive of the Australian Government's work on Horizon 2 to scale cyber maturity across the economy; however, we encourage consideration of ongoing critical gaps in Australia's regulation of cyber security in the renewable energy sector, particularly in Australian homes. More than 4 million households and small businesses across the country have now installed rooftop solar systems[1], and the recently introduced Federal Cheaper Home Batteries Program has seen over 19,500 battery installations in the first month[2].

Australia's electrification journey is just beginning, however. The least-cost pathway to meeting Australia's renewable energy and emissions targets, as modelled in the Australian Energy Market Operator's 2024 Integrated System Plan (ISP) Step Change scenario, requires four times more rooftop solar, 34 times more distributed battery capacity and 135 times more orchestrated battery capacity by 2050[3].

As outlined in the discussion paper, the internet connectivity of consumer and distributed energy resources (CER/DER) exposes the energy system to cyber threats and highlights the need to consider if adequate protections are currently in place to protect Australian households and businesses. A secure energy system, with enhanced cyber security of CER will ensure the energy transition can be achieved with minimal risks to consumers.

Additionally, when planning for scaled cyber maturity across the economy, it is essential that regulatory frameworks for cyber security in the renewable energy sector consider differences in coverage across categories of technologies:

---

[1] rooftop-solar-and-storage-biannual-report_final.pdf
[2] Strong solar battery uptake in first month | Clean Energy Regulator
[3] powering-homes-empowering-people-cer-roadmap.pdf

- Large-scale generators and batteries (above 30MW)
    - Covered by the Security of Critical Infrastructure (SOCI) Act with enforcement variable depending on the industry.
- Medium-scale generators and batteries (less than 30MW but larger than Internet of Things (IoT devices)
    - No current policy or legislation.
- IoT devices, such as consumer and distributed energy resources (CER/DER)
    - Covered by the Cyber Security Act.
- Virtual Power Plants (VPPs), aggregators and original equipment manufacturer (OEM) portals
    - No current policy or regulation.

It is critical that Australian cybersecurity requirements, particularly for the CER/DER, are in line with global best practice to reduce system security risks and vulnerabilities and protect the energy sector, given the high penetration of rooftop solar. Safeguards around these products and their corresponding information networks accessing and controlling them are essential.

While cyber regulation and policy are currently in place, gaps exist in understanding of the application of requirements, their enforcement and reporting. Hence, the CEC is supportive of a clear governance structure around the rules and regulations to achieve domestic and international cyber regulatory alignment. This should clearly define industry-specific arrangements, including private sector partner obligations, duties and responsibilities and have a body in place to administer implementation deadlines and enforce requirements. For the CER/DER sector, it is recommended that publicity around requirements and changes be coordinated through the National CER technical Regulator, as part of the technology workstream in the National CER Roadmap[4].

Recommended Reforms

The CEC outlines the following additional recommendations for IoT devices, such as consumer and distributed energy resources:

- While the SOCI ACT is fit for purpose, the definition of critical infrastructure should be considered to accurately encapsulate the CER/DER sector and the multiple digital connection points into the energy system.
- Consider the inclusion of the entirety of EN 303 654 under the requirements of the Cyber Security Act.
- Consider the introduction of a routine compliance mechanism, this could be attached as an eligibility requirement under the Small-scale Renewable Energy Scheme (SRES).
- Explore the development of a national set of Device, Data, Visibility, Control and Network standards and procedures in the CER/DER industry, managed under a robust governance framework.
- Introduce a cybersecurity certification and labelling program to highlight risk through both hardware and software listing and ranking, allowing entities to understand intrinsic levels of safety existing with products.
- Consider the introduction of permanent Australian representation within the IEC Standards committees, supporting the development and adoption of Standards in Australia.

---

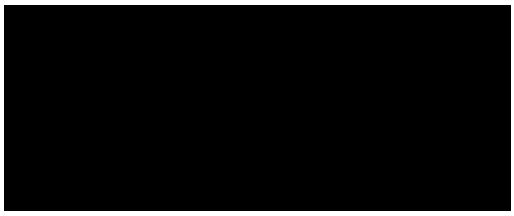
[4] National Consumer Energy Resources (CER) Roadmap - Consultation on technical priorities - Department of Climate Change, Energy, Environment and Water

The following recommendations consider existing gaps in additional renewable energy technology categories and their relevant regulation:

Technology Category	***Recommendations***
Large-scale generators, batteries and aggregated resources (above 30MW)	• Consider modification of the SOCI Act to clarify that fleets of aggregated resources greater than 30MW will still have the 30MW threshold apply, despite no individual generator/battery exceeding 30MW. • Ensure generators and transmission network service providers clearly report on how cyber obligations are passed down the supply chain or ensure this is directly captured by supply chain stakeholders within the SOCI Act.
Medium-scale generators and batteries (less than 30MW but larger than Internet of Things (IoT devices)	• There are currently no regulations for cybersecurity within this size range, yet as the number of commercial and industrial assets in this range grows, associated risk increases. We encourage the Department of Home Affairs to consider a reduction in the threshold of the SOCI Act below 30MW. The new threshold could be informed by the loss of inverter control over the public internet; however, this may vary in jurisdictions due to individual distribution network service provider (DNSP) approaches.
Aggregators, VPPs and OEM portals	• Introduce mandatory standards for VPPs and OEM portals, it is recommended that ISO 27001 could provide an appropriate base line for the initiation of this work.

The Clean Energy Council welcomes further opportunity to discuss the recommendations in this response with the Department of Home Affairs. If you have any queries or would like to discuss the submission in more detail, please contact [redacted]

Kind regards,



[redacted]

Clean Energy Council