Anna Collyer
Chair
Australian Energy Market Commission
Level 15, 60 Castlereagh Street
Sydney NSW 2000
Lodged via https://www.aemc.gov.au/contact-us/lodge-submission

7. November 2024

Dear Ms. Collyer,

Re: ERC0388: Cyber security roles and responsibilities

Vestas welcomes the opportunity to provide our feedback on the AEMC's Draft Rule Determination released on 26 September 2024 regarding AEMO's proposed roles and responsibilities on cyber security matters.

Vestas' vision is to become the global leader in sustainable energy solutions, and everything we do revolves around the development and deployment of these solutions.

We want to express our general support for AEMC's Draft Rule Determination under consultation and offer feedback based on our global experience as a market leader in developing and implementing cyber security systems into our infrastructure, as well as working closely with energy regulators and market operators to ensure resilience against cyber-attacks, as follows:

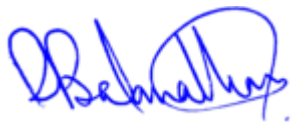
- Regulation should be agnostic to technology and abstain from detailed requirements for technologies and components, thereby allowing for innovation and avoiding rapid obsolescence.
- Regulation focusing on descriptive technical controls may be easily auditable. However, it will lead to sub-optimal risk management. By requiring that stakeholders share information on cyber risks, authorities are given an opportunity to address aspects of national security as they evolve.
- An efficient transition to renewable energy demands that Registered Participants can act risk-informed, with obligations to support national efforts (SOCI Act[1]). Therefore, it is not beneficial to introduce detailed technology requirements.
- Collaboration between the parties involved in the power plant operation, such as generators, network operators, AEMO and Original Equipment Manufacturers (OEMs), including the risk analysis process, should be fostered. It would be beneficial for all parties to introduce incident response frameworks, such as the ICS4ICS[2], as this will effectively enhance response capabilities.
- AEMO should adopt a risk management approach to address Registered Participants' cyber security risks.
- AEMO should define a threshold for criticality based on assessing the power plant's risk or power plant portfolio's risk to the electricity system and not on the size of the owning entity.

[1] Security of Critical Infrastructure Act 2018
[2] Incident Command System for Industrial Control Systems

- Operators of power plants exceeding the criticality thresholds should be required to conduct a risk assessment covering the operational lifetime. This risk assessment shall include risks arising from cyber-attacks on the supply chain (OEM) and the service provider.
- Power plants exceeding the criticality threshold shall describe technical factors for their cyber security. These descriptions may include a software bill of material for plant SCADA solutions (control systems), defined communication protocols to service the plant, and defined inventories for software allowed.
- Vestas supports the Draft Rule Determination in guiding AEMO to effectively engage with relevant government agencies and industry bodies to assist Registered Participants in improving their cyber security preparedness and maturity level. However, the rules should also include OEMs and service providers in such a group.

Should you wish to discuss any aspect of our comments, please contact Marco Aurelio Lenzi Castro at mlzto@vestas.com, 0488 152 925, or the undersigned.

Yours sincerely
Vestas - Australian Wind Technology Pty. Ltd.



Dr Ragu Balanathan
Vice President, Power Plant Solutions
Vestas Asia Pacific
rabln@vestas.com
M: 0439630289