

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>

Melbourne, 18. July 2024

Dear Ms. Collyer,

**Re: ERC0388: Cyber security roles and responsibilities**

Vestas welcomes the opportunity to provide our feedback on the AEMC's consultation paper released on 20 June 2024 regarding new proposed roles and responsibilities for AEMO on cyber security matters.

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

Digitalisation and interconnectivity of energy assets is a prerequisite for a sustainable transformation of the energy sector but comes alongside increasing risk of cyber-attacks. Hence, safeguarding energy systems, against security vulnerabilities requires all stakeholders to adhere to evolving international and national cyber security requirements to support the manufacturing, management, and operation of critical energy infrastructure.

We would like to express our overall support for this rule change request proposed by the Honourable Chris Bowen MP, Minister for Climate Change and Energy, with the aim to specify and amplify AEMO's duties in the National Electricity Rules (NER) on cyber security matters.

Vestas is a market leader in developing and implementing cyber security systems into its infrastructure and works closely with energy regulators and market operators to ensure resilience against cyber-attacks.

We understand that the security and resilience of the electricity system cannot be provided by focusing solely on technology. System security depends on the interplay between all connected entities, assets, and coinciding components.

Vestas is already supporting the development of an open-source cyber risk management framework that allows risk information exchange across the value-chain of the renewable industry.

Based on our global experience, we would like to offer the following recommendations for AEMC on setting new standards for cyber security in the NEM:

- It is more efficient and future-proof to regulate processes than technology.
- The complexity of the value chains requires that there is a framework for collaboration between suppliers, operators, and authorities.
- National security specific risks to society (foreign investments/technology control) should be assessed and addressed by AEMO in consultation with the Department of Foreign Affairs and Trade, the Foreign Investment Review Board, the Australian Security Intelligence Organisation,

and other government agencies tasked with protecting Australians and the Australian energy system from cyber threats.


- The rules should adopt a risk management approach to address market participants cyber security risks.
- Clear definitions are essential for effective governance, regulatory compliance, and collaborative efforts to enhance cyber security resilience across stakeholders.
- AEMO should not have the power to impose mandatory obligations on market participants and Original Equipment Manufacturers (OEMs) regarding cyber security matters.
- Market participants should be responsible for their own cyber security needs and risk control should reside by the ones with the production license.
- The Incident Command System for Industrial Control Systems (ICS4ICS) framework should be adopted by manufacturers, market participants and network operators in Australia.
- OEMs play a key role in ensuring the strength and resilience of their own cyber-security systems and AEMO should continue to work closely with OEMs and other trusted market participants to ensure a resilient and secure energy system.

Please refer to the appendix for our responses for each question presented on the consultation paper.

Should you wish to discuss any aspect of our comments, please contact Marco Aurelio Lenzi Castro via [mlzto@vestas.com](mailto:mlzto@vestas.com) or 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  
[rbln@vestas.com](mailto:rbln@vestas.com)  
[M: 0439630289](tel:0439630289)

## **Appendix: Responses to the consultation paper questions**

### **Question 1: Do you agree that the specific cyber security activities being undertaken on an ad hoc basis is problematic?**

Vestas agrees that cyber activity being undertaken on an ad hoc basis is problematic due to lack of consistency, increasing the risk exposure. In addition, without a coherent strategy, it is difficult to scale and manage effectively and organisations may end up with a fragmented security response.

But there is also a requirement to upgrade legacy operational technology (OT) environment so that a more structured and a proactive approach to cybersecurity practices can be applied.

We would like to highlight some comprehensive approaches taken by energy operators in the EU, such as:

- the Cyber Resilience Act,
- the amendments to the Data Security Act,
- member states' implementation of the NIS2 Directive,
- the Directive on the Resilience of Critical Entities (CRE),
- the introduction of an EU-wide certification framework, and
- the development of the Network Codes on sector-specific rules of cross-border electricity flows.

### **Question 2: Do you consider there is a lack of clarity on the specified roles and responsibilities of cyber security in the NER?**

Yes, the requirements related to cybersecurity roles and responsibilities are subject to interpretation and makes it challenging for organisations to align the practices effectively.

### **Question 3: Would the industry value more cyber security guidance in the NER, why/why not? If yes, what kind of guidance specifically?**

Yes, this can enhance the overall resilience and ensure a co-ordinated approach to cyber security efforts and ultimately safeguarding critical infrastructure against emerging cyber threats.

### **Question 4: Do you agree that the lack of clarity regarding the identified cyber security functions in the rules is problematic? Why or why not?**

Yes. The lack of clarity regarding cyber security functions in the rules can lead to a misunderstanding on roles and responsibilities, inefficient resource allocation, compliance risks, and challenges in incident response coordination.

Clear definitions are essential for effective governance, regulatory compliance, and collaborative efforts to enhance cyber security resilience across stakeholders.

### **Question 5: Do you consider cyber security a power system security issue, a network planning and expansion issue, or neither? Why/why not?**

Power systems are interconnected with various networks including control systems, communications networks and consumer devices. Any vulnerability or other cyber threat in the interconnected networks can potentially affect the power system operations.

Therefore, it is critical to consider cyber security as an integral part of both power systems security and network planning and expansion.

**Question 6: Do you consider that the benefits for clarifying the cyber security incident coordinator as a function for AEMO in the rules outweigh the costs/risks? Why/why not?**

Designating AEMO as the cyber security incident coordinator for the energy sector offers clear benefits. It provides defined responsibility, improves coordination during incidents, strengthens sector preparedness, and ensures compliance with regulations.

However, challenges include allocating resources effectively, managing stakeholder complexities, and avoiding role overreach. Overall, if managed well with sufficient resources and clear guidelines, the benefits of enhanced coordination and preparedness are likely to outweigh these challenges.

**Question 7: Do you consider clarifying the supporting cyber preparedness and uplift as a function in the rules outweigh the costs/risks? Why/why not?**

No comments.

**Question 8: Do you consider the benefits of clarifying the examining risks and providing advice to government and industry as a function in the rules outweigh the costs/risks? Why/why not?**

Australia's energy sector could only benefit from having direct and clear advice provided to government on cyber security risks to the energy system. The nature and form of risks to the Australian cyber security sector will change over time and requires constant monitoring and assessment, and AEMO is well placed to both assess that risk and provide regular updates to government. The nature of the advice should cover risks present across all participants in the energy system.

It is important to note, however, that OEMs play a key role in ensuring the strength and resilience of their own cyber-security systems and thus AEMO should continue to work closely with manufacturers and other trusted market participants to ensure a resilient and secure energy system for all Australians.

As discussed above, the protection and resilience of energy systems cannot occur in a silo. AEMO should be working closely with colleagues in the Foreign Investment Review Board and other government agencies tasked with protecting Australians and the Australian energy system from cyber threats. This will ensure the most comprehensive protection from cyber security threats, and the most complete view of cyber security protection.

**Question 9: Do you consider the benefits of clarifying the facilitating the distribution of cyber security information to market participants as a function in the rules outweigh the costs/risks? Why/why not?**

Clarifying the function of facilitating the distribution of cyber security information to market participants can bring significant benefits such as timely threat awareness, enhanced collaboration, and regulatory compliance. However, it requires careful resource allocation, robust data security measures, and effective coordination to mitigate risks associated with information dissemination and ensure its effectiveness in strengthening cybersecurity resilience across the sector.

It's pivotal to highlight that OEMs and service providers are well equipped and can support AEMO to distribute critical cyber security information to customers

**Question 10: Do you agree with the proposed assessment criteria? Are there additional criteria that the Commission should consider or criteria included here that are not relevant?**

Vestas recommends the inclusion of outcomes for consumers and flexibility to the assessment criteria, once the Final Rule change is expected to strengthen the energy security, benefiting consumers, and provide flexibility to market participants and OEMs to manage their own cyber security needs.