Anna Collyer
Chair
Australian Energy Market Commission

Submitted via website

Dear Ms Collyer,

ENA submission to the Hon. Mr. Bowen's Cyber security roles and responsibilities rule change request

Energy Networks Australia (ENA) welcomes the opportunity to provide input to the Honourable Mr. Bowen's Cyber security roles and responsibilities rule change request.

ENA is the national industry body representing Australia's electricity transmission and distribution and gas distribution networks. Our members provide more than 16 million electricity and gas connections to almost every home and business across Australia.

Cyber security is a critical issue for the Energy industry now and in a high-CER (Customer Energy Resource) future. The decentralised nature of the future grid is one that is inherently harder to secure because it presents a much broader "threat surface" for malevolent actors. Addressing this risk requires coordination across industry which AEMO is well placed to provide.

This new paradigm requires the industry to think differently about how we secure critical infrastructure that also acknowledges the role customers play as an integral part of the generation mix now and into the future.

Key messages

» We agree that AEMO is well placed to play a critical role in cyber preparedness and event response, and broadly support the proposal
» There must be a balance of appropriate investment and capability, not capability at any cost.
» Networks will also require similar uplift in capability now and into the future

Energy Networks Australia www.energynetworks.com.au
Unit 5, Level 12, 385 Bourke Street Melbourne VIC 3000
P: +61 3 9103 0400 E: info@energynetworks.com.au
Energy Networks Association T/A Energy Networks Australia
ABN: 75 106 735 406

AEMO has a clear role in cyber security for Energy

ENA and our members broadly support the rule change proposal to increase AEMO's role in the area of cyber security. We believe they are well-placed to be the central point of coordination for Cyber preparation, information sharing and event response for the Energy industry.

Noting that Cyber incidents are also the domain of various other Federal Government departments and agencies, it is important for a clear set of roles and responsibilities to also be defined in how AEMO and the wider industry interacts and engages with these bodies now and into the future.

For example, Distribution Network Service Providers (DNSPs) must currently support AEMO in ensuring power system security either directly or through delegations from the relevant Transmission Network. DNSPs also have responsibilities to the Department of Home Affairs under the Security of Critical Infrastructure (SOCI) Act.

In the event of a cybersecurity event, networks would need clarity on whose instructions networks would follow first and how our obligations to different authorities and overlapping legislations would be prioritised.

Needs & investment must be balanced

Noting the consequential impact to market participant fees, ENA supports AEMO's ability to uplift their cyber security capabilities only to the extent that it meets the required need and their obligations.

Prudent and efficient investments should be assessed and made in line with the current or expected near-term risks and AEMO's costs in this area will need appropriate oversight and approval to ensure that market participants do not pay for unnecessary or duplicated services in the areas of existing communications channels with bodies such as the Cyber and Infrastructure Security Centre (CISC).

We strongly encourage AEMO and CISC to work together to streamline and delineate communications to market participants to the maximum extent possible.

A rigorous cost benefit assessment must be undertaken to inform a business case justification for AEMOs cyber capability requirements and uplift. To give industry comfort that prudent and efficient costs are being made by AEMO we strongly suggest that these business cases be presented to AEMO-hosted industry engagement groups such as the Financial Consultative Committee (FCC) or similar.

One of the FCC's stated objectives[1] is to "grow stakeholders' understanding of the budget and fee impacts of AEMO's evolving roles and responsibilities" which suggests

[1] https://aemo.com.au/en/consultations/industry-forums-and-working-groups/list-of-industry-forums-and-working-groups/financial-consultation-committee

that this may be an appropriate vehicle by which to build industry support and acceptance of AEMO cyber security costs.

Networks also have an important role in cyber security

Much of what is in the original rule change request can also be applied to Transmission and Distribution Networks. As the operators of the physical networks in which digitised and connected CER operates, it will also be necessary for Networks to have cyber capabilities to secure these operations. On this basis, we recommend the AEMC consider clarifying the role of networks in managing cyber security risks in the rules.

Networks must also ensure that they are compliant to multiple levels of state and federal legislation and ask that the AEMC also consider the network's associated cost of compliance to be included in the cost benefit assessment for any new regulatory change.

We support AEMO's need for funding certainty and believe that Networks should also be afforded a similar level of consideration in their price reset determinations with the Australian Energy Regulatory (AER) to support the operation of a cyber-secure CER future.

If you have any questions or would like to discuss specific topics further, please do not hesitate to contact Dor Son Tan, Head of Distribution Networks dstan@energynetworks.com.au.

Yours sincerely,

Dominic Adams

General Manager Networks