Dear Nomiky Panayiotakis

We thank you for the opportunity to provide a submission for the cyber security roles and responsibilities consultation paper for the rule change request.

The Smart Energy Council (SEC) is the peak independent body for Australia's smart energy industry, representing over 1,300 residential, commercial, and large-scale renewable generation and storage companies, smart transport firms, as well as the renewable hydrogen and ammonia industry.

The Smart Energy Council has recently established a cyber security working group to collaborate on advancing the smart energy industry in the areas of governance, policy, and regulation of cyber security. Our focus is on creating regulation and rules essential for the industry's cyber security journey. We have had strong engagement across various industry sectors, and we welcome this rule change as a significant step forward in strengthening Australia's energy security.

There is a broad consensus on the need for significant reforms to gain a clearer understanding of the cyber security landscape, requirements, and the roles of government entities operating in this space. We welcome more engagement with the industry to ensure the development of fit-for-purpose solutions, including adhering to international standards where possible.

Our core recommendation is that the government adopts a proactive approach to cyber and energy security. This should be a step towards the comprehensive development of cyber security for Australia's energy market.

Should you wish to discuss any of this submission further, please contact:
Wayne Smith, External Affairs Manager, Smart Energy Council
(02) 6241 0171
Wayne@smartenergy.org.au

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

Yes. There needs to be a coordinated strategy to build and maintain cyber security across the energy network to prevent and minimise the impact of cyber attacks. There should be a comprehensive development of cyber security for Australia's energy market where the responses need to be risk based and a scaled response. Identification of risks must be for each sector ie: CER will differ from C&I which will differ from utility grid based assets (which might still be on the distribution networks). The balance is to assess & deal with risks which have system wide potential impacts, not those which might simply affect one or even a few consumers.

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 National Electricity Rules (NER) currently lack clear specifications regarding cyber security responsibilities.

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

Yes. Comprehensive guidance is necessary for consistent operation across different organizations.

Distributed Network Service Providers (DNSPs) are developing their own cyber security rules due to a lack of clarity from market operators and government entities, leading to variability across jurisdictions. More direction is needed to ensure consistent national rules, especially across the National Electricity Market (NEM).

High-risk industries, such as utilities, desire frameworks with minimum cyber security requirements. The Security of Critical Infrastructure Act 2018 (SOCI) classifies critical infrastructure as above 30 MW, yet there are no cyber security requirements in the NER for anything below 30 MW.

PO BOX 231, MAWSON ACT 2607
INFO@SMARTENERGY.ORG.AU
SMARTENERGY.ORG.AU

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 NER does not mention cyber security functions, which is problematic and we welcome the proposed rule change.

Notably, we encourage that the focus should be on making the entire system more resilient, not just on incident response. Proactive government action is required to ensure energy security, and support is needed throughout the market for preparedness.

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

Cyber security is all of these and more. It should be integrated to network planning and expansion, and cyber security instigates issues, caused by a lack of planning and well-built systems. The outcomes of a cyber security incident is a power security issue. Network expansion becomes a planning issue when building in redundancy.

The market may not see robust cyber security as worthwhile when planning and expanding networks, so there is a clear requirement for the government to outline a clear minimum standard and have it enforced consistently across jurisdictions.

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?

Yes. AEMO has the skills and is already starting down the path of becoming the cyber security incident coordinator.

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?

Yes, absolutely. Strengthened cyber security and preparedness is even more than a network planning and power system security issue. It is a national security issue, as well as a customer privacy issue and should be regarded as such when weighing-up a cost/risk analysis.

PO BOX 231, MAWSON ACT 2607
INFO@SMARTENERGY.ORG.AU
SMARTENERGY.ORG.AU

There is a lack of clarity around the communication, education and information activities, regarding who pays for and delivers these. The incumbents, including large utilities, are all well funded and resourced with many having guaranteed revenue streams (RAB & other regulated income, etc.), yet the new rules are likely to be imposed largely on the new players, being renewables. These are largely capital expenses that will have whole of system benefits, but paid for by first into the market. If this is the intended model then tax breaks or other government support needs to be made available.

It must be noted that costs are carried eventually by consumers. The risk assessments need to be very clear about the benefits and costs on who is expected to pay for these changes.

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?

Yes. Clearly providing the government with advice is the cheapest and most cost effective approach. It must be stressed that there should be industry involvement in this process, with a collaborative approach taken beyond submission processes such as these.

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?

Yes. This will provide value for the industry and a collaborative, information-sharing approach is encouraged.

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?

Broadly, yes. However, there should be international considerations to ensure consistent implementation across jurisdictions.

PO BOX 231, MAWSON ACT 2607
INFO@SMARTENERGY.ORG.AU
SMARTENERGY.ORG.AU