Thursday, 18 July 2024

Australian Energy Market Commission
Level 15, 60 Castlereagh Street
Sydney, 2000, NSW

ERC0388 Cyber security roles and responsibilities consultation paper

Dear Ms Panayiotakis,

The Clean Energy Council (CEC) is the peak body for the clean energy industry in Australia, representing nearly 1,000 of the leading businesses operating in renewable energy, energy storage, and renewable hydrogen. The CEC is committed to accelerating the decarbonisation of Australia's energy system as rapidly as possible while maintaining a secure and reliable supply of electricity for customers.

We welcome the opportunity to comment on the proposed rule that seeks to clarify the role of AEMO in cyber security under the *Cyber security roles and responsibilities consultation paper*.

The CEC considers that the four functions being proposed under the rule change are reasonable, building on existing activities. We agree that AEMO should formally have the coordinator role defined. Market participants benefit from having clear direction when following cyber security procedures, especially since these apply differently to different levels of the energy supply chain.

The CEC proposes that the role of cyber security for AEMO is specifically defined in the NER as part of the power system security function. AEMO has the responsibility and authority of issuing system security directions, prepare a system restart plan for managing and coordinating system restoration during a major disruption, and coordinate the protection of power system equipment. A cyber incident would have a similar effect as a system-wide disruption. We also draw attention that consumer resources that can be aggregated to dispatch in the NEM as Integrated Resource Providers relate to cyber security of Internet of Things and currently falls out of scope.

The CEC also acknowledges that these additional functions come at a cost. Distribution network providers already add cyber security uplift to their revenue determination to the AER[1]. The industry stands to benefit from more cyber security scrutiny and coordination. As seen with other sectors, the price of not taking cyber security seriously is too great.

As the energy system evolves, several key areas could be vulnerable to cyber attacks[2]:

[1] AusNet, 2024, Business case: ICT Non-Recurrent – Cyber Security Uplift, 2025-30 Regulatory Proposal and Energex, 2024, Cyber security Business base

[2] Energy Networks Australia, 2023, Cyber Security and Energy Networks

- The grid network and its components such as substations, transformers and the systems used to control them
- The generator assets and the cloud systems supporting their interface with the grid
- The private and commercially sensitive data of participants
- The integration of distributed technologies and supporting systems such as consumer energy resources network communication systems and virtual power plants

How these systems are integrated to respond to any cyber incidents requires much needed compliance, guidance, and governance. The Security of Critical Infrastructure (SoCI) Act has elevated the compliance of cyber security within the energy industry with a set of obligations placed on market participants. This has also led developers, OEMs, and transmission and distribution networks to adapt the SoCI Act to fit their purpose, with unclear understanding of responsibilities of different market participants. For example, only a subset of obligations applies to OEMs, but developers are not aware which. OEMs in turn, appeal to extra services from consultants to identify these obligations in an effort of not taking on unnecessary risk.

Guidance however is well underway and AEMO's role as coordinator will continue to set standards for market participants. The Australian Energy Sector Cyber Security Framework (AESCSF) prepared by AEMO offers market participants information on how to:

- Use the self-assessment results to inform actions, priorities and investments to deliver a consistent risk-based approach to building operational resilience
- Benchmark their organisation against energy sector peers
- Assess their cyber maturity to support their Risk Management Plan (RMR) regulatory obligations under the SoCI Act
- Inform content for the Cyber Security Preparedness of the Australia's Energy Sector Annual Report which in turn informs sector policies to improve cyber security and operational resilience
- Speak a common cyber language and work collaboratively

The AECSCF is a useful starting point. There are multiple parts that add value to the self-assessment tool such as defining the domains, maturity levels, and security profiles. This information is then used by AEMO (once anonymised) to prepare the Cyber Security Preparedness of the Australia's Energy Sector Annual Report. This role is critical for both cyber security coordination and response in case of a cyber security incident. However, with increasing sophistication and digitisation of the energy market, it is crucial to solidify AEMO's role. The CEC agrees that ad-hoc cyber security activities are problematic. Despite the breath of scope outlined in the AECSCF, it remains unclear who develops guidelines that apply to each market participant.

Most notably, a lack of a cyber security governance framework poses a risk. Currently, practices are reactive, with improvement opportunities driven from a compliance perspective (such as the SoCI Act). With the evolving nature of power system controls and distributed resources, threat detection requires continuous monitoring to detect any malicious activities. Cyber security event monitoring is indispensable for protecting the power system. Such activities require skilled personal and dedicated resources, which largely falls on each generator, network operator, and retailer. However, AEMO's function as aggregator of NEM-wide information on cyber security will go a long way in addressing blind spots. We argue that a structure of decision-making, processes, and a common language are essential to building trust and cohesion of security objectives. Clarity will help drive cyber security investment. Although the question of governance is out of scope for this rule change, we support AEMC in further work that brings together different streams of work related to cyber security issues.

As always, the CEC welcomes further engagement from the AEMC on this reform in the following steps of the rule change. Further queries can be directed to Ana Spataru at the CEC on aspataru@cleanenergycouncil.org.au.

Kind regards

Christiaan Zuur
Director, Market, Investment and Grid