Dear Nomiky Panayiotakis,

18.07.2024

Rule Change Request Submission
Australian Energy Market Operator – Cyber Security Role

Fronius has a vast 75 years of experience in industry and known as a leading premium solar inverter OEM in the residential and commercial sector of Australia. In the last ~6.5 years alone we have sold 3.5GW of inverters to be connected to the Australian grid. As per regulations, we are also facilitating remote control of hundereds of MW's of Fronius inverters in Australia as a service to DNSP's. With 38 subsidiaries globally and employing over 5000 staff we take this industry seriously and welcome the idea of considering this new cyber role and its responsibilities.

With regards to cyber, Fronius is based in Austria which includes our manufacturing and R&D, hence we are already conforming with a plethora of cyber rules/regulations including GDPR and ISO27001. We hope there will be some international recognition and consideration in Australian cyber advice for the various frameworks we already need to comply with in the EU.

The main topics we see as lacking with regards to responsibilty of cyber regulation are as below:

Clarity on requirements for large scale CER control in legislation:

Fronius emphasizes the need for clear cybersecurity guidance and leadership to enhance protection measures of Australia's power system in both the residential and commercial sector. We believe the current framework has a looming expectation of change, particularly regarding the classification of 'critical assets/components' for inverters, EV chargers and aggregator cloud services under the SOCI act. Presently, SOCI classifies electrical plants exceeding 30MW as critical electricity assets. However, for example, aggregated control of 500MW's of CER is not clearly included within any SOCI classification. Importantly, there is no direct responsibility for cyber in this space as these types of assets are not directly captured under SOCI. This lack of clarity as to when and what we are required to do from a cyber perspective is problematic in our buisness operations. We have no way to prepare for requirements that could take years to fufill but may come into effect sooner than we can act.

Cyber Requirements for VPP's and national Approach for DNSP Cyber requirements:

Currently, there are no clear cyber rules/responsibilities in the space of VPP's and DNSP rules are individually creating cyber requirements for devices under their control. These rules potentially entale significant buisness changes for OEM's as each DNSP creates there own cyber necessities. Without a national approach, this again poses significant challenges for Fronius in planning for future cybersecurity needs.

Fronius Australia Pty Ltd
90-92 Lambeck Drive
Tullamarine VIC 3043
ABN 65 144 615 896
T: +61 3 8340 2900/F: +61 3 8340 2909
pv-sales-australia@fronius.com
www.fronius.com

Varied requirements and constantly changing cyber landscape for OEM's:

Individual companies, government bodies and DNSP's approach Fronius with their own unique cybersecurity requirements to fulfill there own interal requirements, SOCI obligations, etc.. This again highlights the need for a cohesive national strategy which includes the OEM. As Virtual Power Plants (VPPs) and DNSPs remote control (via CSIP-AUS) gain prominence through market and necessity, a national cybersecurity framework specifically addressing this domain is essential for protection across Australia's energy infrastructure.

Responses to the questions in the consultation paper from Fronius' perspective:

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

Yes. Having cyber activities undertaken on an adhoc manner sounds similar to waiting for a problem to happen and then overreact causing huge costs to the industry. We must have a national cohesive strategy layed out for the future of remote CER control as it takes large buisnesses time to adjust and plan, doing this in an adhoc manner is typically not suitable.

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

Yes. As outlined above, large scale CER control for grid services and retailers seems to have no clarity on what will cyber regulation will come or what should be currently applied.

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

Yes. There should be a national approach for DNSP rules and VPP control when reaching a certain threshold of MW's of CER control which is relevant to the national security of the country.

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 energy sector is clearly important to everyone in the nation and I don't see any reason to retain a lack of clarity.

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

My comments pertain to power system security specificialy, especially when buisnesses can control hundreds of MW's of generation with no cyber regulation. However I believe that network planning and expansion would also include controllable CER and is integral to a strong electrical grid especailly as the residential sector further electrifies.

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?

I would think that clarifying cyber security is a topic where the weakest link in the chain can break the entire system. It is crutial to ensure that the responsiblities are clear in this sector as a matter of national security.

Fronius Australia Pty Ltd
90-92 Lambeck Drive
Tullamarine VIC 3043
ABN 65 144 615 896
T: +61 3 8340 2900/F: +61 3 8340 2909
pv-sales-australia@fronius.com
www.fronius.com

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?
Costs to clarify cyber prepedardness should not cost more than the damage dealt from having existing open issues taken malicious advantage of (e.g. power system instability/outage).

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, providing advice seems like a cost effective way to mitigate the broader risk. There should definietely be government involvement, especially regarding a national approach for DNSP's.

Please reach out to me for further discussions or clarifications of our concerns.

Best regards,

Geordie Zaphiris

Solutions Engineer

Mobile: +61 (0) 424 751 312

Zaphiris.Geordie@fronius.com

Fronius Australia Pty Ltd
90-92 Lambeck Drive
Tullamarine VIC 3043
ABN 65 144 615 896
T: +61 3 8340 2900/F: +61 3 8340 2909
pv-sales-australia@fronius.com
www.fronius.com