SMA Australia Pty. Ltd.
ABN: 44 127 198 761
Level 1, 213 Miller Street
North Sydney NSW 2060
Tel.: +61 1800 SMA AUS
www.SMA-Australia.com.au

18 July 2024

Anna Collyer
Chair
Australian Energy Market Commission
Level 15, 60 Castlereagh St
Sydney 2000
E: aemc@aemc.gov.au

Consultation feedback on Cyber Security Roles and Responsibilities in the NEM

Dear Ms Collyer,

Thank you for the opportunity to provide feedback to the Australian Energy Market Commission (AEMC) Consultation Paper on Cyber Security Roles and Responsibilities in the National Electricity Market (NEM).

As a leading global specialist in photovoltaic (PV) system technology, SMA is setting the standards today for the decentralized, digital and renewable energy supply of tomorrow. Our product range spans the home rooftop sector, commercial and industrial applications, and large grid-scale applications. Our product range includes grid-connected inverters, inverters for independent, stand-alone systems and storage solutions for battery systems of all sizes. Our PV solar inverter and battery storage products are complemented by components for energy management, system monitoring, and data analysis. SMA has a global inverter capacity of 140 GW in more than 190 countries and more than 9GW inverter capacity in the Australian market. We are headquartered in Germany, with more than 4,300 SMA employees in 20 countries and over 110 employees across Australia.

SMA plays an active role in development and implementation of cyber security policies, regulations and standards. As a supplier of inverters to utility-scale generators, SMA-Australia has achieved SP1 compliance under the Australian Energy Sector Cyber Security Framework (AESCSF). We comply with ISO/IEC 27001, the standard for information security management systems. As an original equipment manufacturer (OEM), SMA has achieved compliance with IEC 62443-4-1 (requirements for the secure development processes of products), IEC 62443-4-2 (requirements for products) and parts of IEC 62443-3 (system security requirements).

We welcome the fact that the Consultation Paper considers cyber security roles and responsibilities in a broad context and has not limited itself to the details of the rule change request. There is an urgent need for clarity in the governance of cyber security in the NEM.

SMA Australia Pty. Ltd.
ABN: 44 127 198 761
Level 1, 213 Miller Street
North Sydney NSW 2060
Tel.: +61 1800 SMA AUS
www.SMA-Australia.com.au

Some key areas in need of resolution include:

- Who is responsible for developing cyber security policy for the NEM?
- What areas of cyber security policy and regulation should sit within the National Electricity Laws (NEL) and National Electricity Rules (NER), and which areas should sit outside the NEL and NER?
- What is the policy rationale for cyber security measures in the NER (e.g. data security, national security, jurisdictional coverage, security of personal data, prevention of corporate espionage)?
- Who is responsible for setting policy for cyber security preparedness in the electricity sector?
- Who is responsible for enforcement of cyber security obligations in the electricity sector?
- Who is responsible for developing guidelines on the application of high-level cyber security principles to specific business models and practices?
- What is the appropriate role for distribution network service providers (DNSPs) and other businesses in developing and enforcing their own cyber security rules?

I have enclosed a submission, which is in a format suitable for publication on your web site. SMA-Australia's head of Energy Policy and Regulation, Darren Gladman, is the chair of the Smart Energy Council's Cyber Security Working Group and he will continue liaising with you on our behalf.

Best regards,

Doris Spielthenner
SMA Australia
Regional Manager APAC & Managing Director Australia & NZ

SMA Australia Pty. Ltd.
ABN: 44 127 198 761
Level 1, 213 Miller Street
North Sydney NSW 2060
T +61 1300 SMA

Feedback on the Cyber Security Roles and Responsibilities Consultation Paper

SMA-Australia welcomes the opportunity to provide feedback to the Australian Energy Market Commission (AEMC) Consultation Paper on cyber security roles and responsibilities.

As a leading global specialist in photovoltaic (PV) system technology, SMA is setting the standards today for the decentralized, digital, and renewable energy system of tomorrow. Our product range spans the home rooftop sector, commercial and industrial applications, and large grid-scale applications. Our PV solar inverter and battery storage products are complemented by components for energy management, system monitoring, and data analysis. SMA has a global inverter capacity of 140 GW in more than 190 countries and more than 9GW inverter capacity in the Australian market. We are headquartered in Germany, with more than 4,300 SMA employees in 20 countries and over 110 employees across Australia.

SMA plays an active role in development and implementation of cyber security policies, regulations and standards. SMA-Australia's head of energy policy and regulation is the chair the Smart Energy Council Cyber Security Working Group. As a supplier of inverters to utility-scale generators, SMA-Australia has achieved SP1 compliance under the Australian Energy Sector Cyber Security Framework (AESCSF). As an original equipment manufacturer (OEM), SMA has achieved compliance with IEC 62443-4-1 (requirements for the secure development processes of products), IEC 62443-4-2 (requirements for products) and parts of IEC 62443-3-x. We are also compliant with ISO/IEC 27001, the standard for information security management systems.

We welcome the fact that the AEMC's Consultation Paper considers cyber security roles and responsibilities in a broad context and has not limited itself to the details of the rule change request. There is an urgent need for clarity in the governance of cyber security in the National Electricity Market (NEM). Some key areas in need of resolution include:

- Who is responsible for developing cyber security policy for the NEM?
- What areas of cyber security policy and regulation should sit within the National Electricity Laws (NEL) and National Electricity Rules (NER), and which areas should sit outside the NEL and NER?

SMA Australia Pty. Ltd.
ABN: 44 127 198 761
Level 1, 213 Miller Street
North Sydney NSW 2060
www.sma.com.au

- What is the policy rationale for cyber security measures in the NER (e.g. data security, national security, jurisdictional coverage, security of personal data, prevention of corporate espionage)?
- Who is responsible for setting policy for cyber security preparedness in the electricity sector?
- Who is responsible for enforcement of cyber security obligations in the electricity sector?
- Who is responsible for developing guidelines on the application of high-level cyber security principles to specific contracts and business practices?
- What is the appropriate role for distribution network service providers (DNSPs) and other businesses in developing and enforcing their own cyber security rules?

SMA Australia Pty. Ltd.
ABN: 44 127 198 761
Level 1, 213 Miller Street
North Sydney NSW 2060

Responses to questions raised in the Consultation Paper

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

Yes.

Currently, it is unclear who is responsible for determining cyber security policy in Australia's electricity sector. The absence of an agreed policy framework has led to the emergence of cyber security rules being set by distribution network service providers (DNSPs), notably SA Power Networks (SAPN), which are enforced through connection requirements. Without reference to an overarching policy framework, interpretation of the SAPN rules is problematic.

Renewable energy developers and generators are beginning to require compliance with the Australian Energy Sector Cyber Security Framework (AESCSF) as a condition of contracts. While it is sensible for developers and generators to pass through some AESCSF obligations to their supply chain, there is only a subset of the AESCSF that logically applies to part of their supply chain. Ideally, there would be agreed guidelines for the AESCSF obligations of plant operators, technology providers, original equipment manufacturers (OEMs) and others. However, such guidelines do not yet exist, and it is unclear who has the responsibility for developing them. In the absence of such guidelines, industry is writing its own. This is clearly undesirable and is likely to lead to different guidelines and interpretations. The lack of a cyber security governance framework for Australia's electricity sector is the root cause of this problem.

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

Yes.

The lack of clarity includes the following:

- There is no agreed governance framework for cyber security in Australia's electricity sector.
- There is no cyber security policy for Australia's electricity sector.
- It is unclear who is responsible for making cyber security policy for Australia's electricity sector.

SMA Australia Pty. Ltd.
ABN: 44 127 198 761
Level 1, 213 Miller Street
North Sydney NSW 2060

- It is unclear whether a government body will develop guidelines for the application of the AESCSF to different parts of the renewable energy supply chain or if it will be left to industry to develop its own guidelines.
- DNSPs are beginning to make their own rules without reference to a policy framework.
- It is unclear whether DNSPs' connection agreements are intended to be the mechanism for enforcing cyber security requirements.
- It is unclear whether the Energy and Climate Change Ministerial Council (ECCMC) will set a new direction for regulation of technical aspects of renewable energy.

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

Yes. Areas where the industry would benefit from cyber security guidance include:

- Governance – who sets cyber security policy for the electricity sector and which areas of cyber security policy for the electricity sector are outside the National Electricity Laws (NEL) or the NER?
- What is the policy rationale for cyber security measures in the NER (e.g. data security, national security, jurisdictional coverage, security of personal data)?
- Clarification that the AESCSF is the primary framework for cyber security compliance.
- Clarification regarding who is responsible for setting policy for cyber security preparedness in the electricity sector.
- What are the proposed enforcement mechanisms for cyber security measures in the electricity sector?
- What is the role for the Australian Energy Market Operator (AEMO) in cyber security preparedness?
- What is the role for transmission network service providers (TNSPs) and DNSPs in cyber security preparedness?
- Who is responsible for developing or approving guidelines on which parts of the AESCSF apply to whom according to the various roles and business models of the company concerned?

SMA Australia Pty. Ltd.
ABN: 44 127 198 761
Level 1, 213 Miller Street
North Sydney NSW 2060
T: +61 1300 30

- What is the regulatory framework for cyber security for generators less than 30 MW?
- What is the regulatory framework for virtual power plants (VPPs), including those that are more than 30 MW in aggregate capacity?

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.

In the absence of clarity regarding governance, policy and regulation of cyber security measures, DNSPs and other companies in the renewable energy supply chain are writing their own regulatory guidelines. There is potential for misunderstanding and disagreement. Writing regulatory guidelines should be a role for government.

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

Cyber security is certainly a power security issue and a national security issue. It is also a data security issue, a corporate espionage issue, and an issue for privacy of customer data.

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.

The cost of one system black failure in the National Electricity Market (NEM) due to lax cyber security would more than outweigh the cost of cyber security preparedness.

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.

SMA Australia Pty. Ltd.
ABN: 44 127 198 761
Level 1, 213 Miller Street
North Sydney NSW 2060

Cyber security preparedness is already occurring; however, it is being implemented in an ad hoc manner. Therefore, we should not compare the costs and benefits of a cyber security framework to the business-as-usual (BAU) scenario of no cyber security framework. The more realistic comparison would be to consider the costs and benefits of a clear, well executed framework versus the BAU scenario of an ad hoc, poorly executed framework.

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.

The costs of providing advice to government and industry would be very small compared with the potential costs of system failure, and the costs that industry is already incurring from an ad hoc approach to cyber security regulation.

This is potentially a national security. Control of our energy system should be exercised from within our national borders. We should not continue to allow electricity generation to be controlled by computer servers that are not onshore.

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

Yes.

Providing information and guidance to market participants is likely to have the most favourable cost-benefit ratio of all the actions under consideration. Industry is already paying for advice from consultants, and we don't know whether consultants are providing conflicting advice or how to determine what advice is 'correct'. A single, verified interpretation of the cyber security framework as it applies within the NER will clarify what industry needs to do and will reduce costs arising from differences of opinion and interpretation within industry.

SMA Australia Pty. Ltd.
ABN: 44 127 198 761
Level 1, 213 Miller Street
North Sydney NSW 2060

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?

Considering the National Electricity Objectives (NEO) and the issues raised in the rule change request, the Commission proposes assessment against the following three criteria:

- Safety, security and reliability
- Principles of good regulatory governance, and
- Implementation considerations.

This is reasonable within the confines of the NEO, however this approach will underestimate the benefits of cyber security because it places 'out of scope' potential benefits such as national security, industrial espionage security, jurisdictional coverage and privacy of customer data.