**Feedback on AEMO’s New Cyber Security Roles and Responsibilities**

SMA-Australia welcomes the opportunity to provide feedback to the Australian Energy Market Operator (AEMO) Consultation Paper on AEMO’s New Cyber Security Roles and Responsibilities.

SMA is a leading global specialist in photovoltaic (PV) system and battery energy storage system (BESS) power conversion and control technology. 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 Australia. We are headquartered in Germany, with employees in 20 countries.

SMA strongly supports the recent initiatives to uplift cyber security in the energy sector, which include:

* The National Electricity Amendment (Cyber security roles and responsibilities) Rule 2024, which formally established AEMO’s cyber security functions, obligations, and powers in the National Electricity Rules (NER),
* The establishment of the Cyber Security Act 2024, and
* The endorsement by the Energy and Climate Change Ministerial Council (ECMC) of a National Consumer Energy Resources (CER) Roadmap including a *Roadmap for CER Cyber Security*.

We would like to take this opportunity to update AEMO on progress recently made by SMA in cyber security.

SMA has worked with cyber security consultants CAPA Intelligence to develop guidelines for compliance with the Australian Energy Sector Cyber Security Framework (AESCSF) applicable to suppliers of inverters to utility-scale generators. The guidelines were completed in June 2024 and by August 2024 SMA had completed a self-assessment to demonstrate SP1 compliance with the AESCSF guidelines. We have subsequently used the guidelines and our assessment against them to satisfy electricity generators who have included cyber security compliance as a contractual requirement for inverter original equipment manufacturers (OEMs). We would be pleased to share the guidelines and our self-assessment against them with you.

In September 2024 we successfully completed our assessment to demonstrate compliance with the SA Power Networks’ *Dynamic Exports Cyber Security Requirements*.

On 9 October 2024 SMA announced that our customer data management portal, known as Sunny Portal Solution and its associated software, hardware and support processes, are certified under ISO/IEC 27001, which is the premier international standard for information security management systems. Compliance with ISO 27001 provides assurance of a high level of cyber security and protection of the privacy of customers’ personal energy data.

**Responses to questions raised in the Consultation Paper**

**PART A – Declared NEM Project**

1. **Do you consider the cyber security roles and responsibilities is a major reform or development of the NEM?**

Yes. The *National Electricity Amendment (Cyber security roles and responsibilities) Rule 2024* explicitly includes the coordination and support of cyber security preparedness, response and recovery as one of AEMO’s power system security responsibilities.

1. **Do you consider the cyber security roles and responsibilities is a major change to an AEMO function, responsibility, obligation or power under the Rules?**

Yes. Cyber security preparedness, response and recovery for the National Electricity Market (NEM) is a significant new addition to AEMO’s functions.

1. **Do you consider the cyber security roles and responsibilities is a major change to the computer software or systems that AEMO uses in the performance of AEMO’s functions, responsibilities, obligations and powers under the NER?**

SMA does not have sufficient information to provide informed comment on the extent to which AEMO’s cyber security roles and responsibilities will affect the computer software or systems that AEMO uses. However, we can observe from our own experience that cyber security uplift can involve significant changes to software and systems and there is no reason to believe that would not be the case for AEMO.

The role for AEMO requiring process design around the governance of the AESCSF and implementation and promulgation of updates is an important and relatively urgent task that will involve new programs and regulatory reforms that will be of a complex nature.

**PART B – Participant Fee Structure**

1. **Do stakeholders agree AEMO should recover AEMO’s costs for the cyber security roles and responsibilities from 1 July 2025 for a period of seven years (pending any different determinations that may be made in the next general NEM Participant fee structure consultation)?**

Yes. The proposal seems reasonable.

**2.a Which, if any, of the above fee structure options are appropriate for the recovery of costs associated with AEMO’s cyber security roles and responsibilities and why or why not?**

It seems reasonable to expand the existing Participant fee structure for costs incurred on and from 12 December 2024. If an additional (separate) cyber security function fee is established, it would be preferable for that to be considered as part of the next National Electricity Market (NEM) Participant fee consultation which would allow for more detailed consideration in the context of other changes to AEMO’s roles and responsibilities, and the costs incurred fulfilling them.

**2.b Is there another fee structure (not presented above) that would be more appropriate for recovering the costs associated with AEMO’s cyber security roles and responsibilities and why?**

A reasonable argument could be made for allocation of AEMO Participant fees to distribution network service providers (DNSPs), especially given the increasing importance of managing the cyber security or consumer energy resources (CER), distributed energy resources (DER) and other distribution network assets and their impact on the bulk power system. However, we support AEMO’s view that, if this is considered, it should be done as part of the upcoming general NEM Participant fee structure consultation for the fee period commencing 1 July 2026.

**2.c Which Registered Participant/s should the costs of AEMO’s cyber security roles and responsibilities be recovered from and why?**

Initially, the allocation could commence with equal attribution of costs of the cyber security roles and responsibilities across Wholesale Participants, transmission network service providers (TNSPs) and Market Customers, with allocation to DNSPs to be considered as part of the upcoming general NEM Participant fee structure consultation.

1. **In relation to example options 1 and 2, are the fee metrics used for the relevant Participant fee structures appropriate to apply to the recovery of costs associated with cyber security roles and responsibilities? If not, what metric(s) is/are more appropriate?**

Cost recovery metrics should be based on a beneficiary-pays principle. Fees should be proportional to the demand for cyber security services placed by relevant participants upon AEMO. When AEMO has several years of experience with implementing its new cyber security roles and responsibilities, it will be better placed to judge where demand for its services is greatest and how to allocate fees fairly and in proportion to the demands placed upon it.