The Energy Security Board
c/o the Australian Energy Market Commission
Level 15, 60 Castlereagh Street
Sydney NSW 2000

Via email

3rd February 2022

Submission on the Assessment Framework to develop Interoperability Policy for Distributed Energy Resources in Australia

Ross Technology Consulting welcomes the opportunity to make a submission to the Energy Security Boards (ESB) Framework to develop Interoperability Policy for Distributed Energy Resources in Australia. Ross Technology Consulting is an engineering management consultancy focused on supporting the energy industry to adapt to the disruptive challenges presented by the introduction of new technologies and also owns Utility Meter Verification Services which is a NATA and NMI accredited energy metering verification laboratory. Doug Ross is our Principal Consultant and Chairs the Standards Australia Electricity Metering Equipment Committee (EL-011).

We have reviewed the Assessment Framework and our submission is focused on commenting on Criterion 1: System Security and Reliability and Criterion 5: Data privacy and cyber security.

We are concerned that the assessment framework is not placing enough emphasis on ensuring adequate standards and legislative instruments exist to ensure the secure operation of the NEM with large amounts of DER.

By secure, we mean that DER infrastructure is not exposed to unwanted centralised control by hostile actors.

For example, most electric vehicle manufactures maintain a connection via the internet to their vehicles either via a consumers Wifi connection or via a mobile phone in the vehicle. If a hostile actor gained access to the manufactures fleet of vehicles, they could instruct the fleet to charge in a manner that destabilises the grid (i.e. all on once on maximum charge). Equally, inverter and battery manufactures whose devices are connected to the internet, could facilitate hostile actors centrally orchestrating their equipment in a manner that destabilises the grid. The same can be said for Smart Metering infrastructure. The South Australia governments Smarter Homes Regulation requires that inverters be directly connected to and controlled via the smart meters. While the current metering service providers take measures to secure their infrastructure, this is not governed by standards to prevent either the service providers themselves or the suppliers of their equipment from allowing access by hostile actors thus facilitating unwanted central control of the connected DER.

As the amount of “connected” DER increases in the grid, the risk that the grid can be destabilised by hostile actors interventions into the control systems of DER manufactures or service providers grows. We understand that some foreign powers actually require by law that manufactures operating within their jurisdiction facilitate government access to their systems if requested. This was illustrated by the Australian Government’s decision to prevent Huawei from participating in the role out of Australian 5G communications networks.

We also note that the Australian government has recently released its Blueprint for Critical Technologies, which details the Australian Government’s framework for capitalising on critical technologies to drive a

technologically-advanced, future-ready nation. The blueprint via its action plan, does identify DER critical technology's and there security as requiring policy development. We would encourage the ESB to ensure that the Assessment Framework to develop Interoperability Policy for Distributed Energy Resources in Australia is appropriately linked to the work being done in the Blueprint for critical technologies.

Should Australia find itself in a conflict with a foreign power, our energy grid may be exposed to disruption if appropriate legislative instruments and standards are not in place to ensure the providers of DER equipment and services have the access to their equipment adequately secured. This may also require that some equipment manufacturers are excluded from the Australian market if they have legal obligations placed on them in their home jurisdiction to facilitate foreign power access to DER infrastructure.

We note that key finding #4 has highlighted the tension between Criterion 5 and Criterion 1 when considering security but in reviewing the framework, the focus seems to be on data security and not grid security. We encourage the ESB to prioritise grid security. It is vitally important that DER is not integrated into the grid in a manor that creates and attack vector for hostile actors to undermine our ability to "keep the lights on". Should you have any questions in relation to this submission please contact Doug Ross on XXXX or doug@rosstechnology.com.au.

You Sincerely

Doug Ross
Principle Consultant