(ACN 154 893 857)

SwitchDin Pty Ltd
Level 1, Building B, 91 Parry Street,
Newcastle NSW 2302

22 November 2022

Anna Collyer
Chair
Energy Security Board
Submission by email to info@esb.org.au

Dear Ms Collyer,

RE: Energy Security Board Interoperability Policy Directions Paper

SwitchDin welcomes the opportunity to provide feedback to the Energy Security Board (ESB) directions paper on interoperability policy.

SwitchDin is an Australian energy software company that bridges the gap between energy companies, equipment manufacturers and energy end users to integrate and manage energy resources on the grid. SwitchDin's technology enables our clients to build and operate vendor-agnostic virtual power plants (VPPs) and microgrids, and to optimise performance across fleets of diverse assets. Founded in Newcastle NSW in 2014, SwitchDin operates in all states of Australia, including in leading-edge distributed energy projects like Simply Energy's national VPP, flexible export programs in South Australia (SA) and Victoria, Project Symphony in Western Australia (WA) and the Solar Connect VPP in the Northern Territory (NT), among others.

SwitchDin works with distribution network service providers (DNSPs), electricity retailers, inverter original equipment manufacturers (OEMs) and aggregators to enable and utilise flexible export capability. We are working closely with several DNSPs, including SA Power Networks, AusNet Services and the Horizon Power Onslow Project, to develop utility servers capable of interacting with CER directly utilising the IEEE 2030.5 protocol compliant utility servers and clients (direct and aggregator) aligned with the Australian modified Common Smart Inverter Profile (CSIP-Aus) implementation guide, capable of interacting with OEM CER directly or via an aggregator cloud service. We also have a gateway device, called a Droplet, which can operate as a IEEE 2030.5 client and we support other interoperability standards and proprietary methods using our Droplet and cloud. Using these capabilities we enable DNSPs to implement flexible export and dynamic operating envelopes and other services, and we enable Traders to access energy markets. This experience gives us a deep understanding of the challenges and benefits of the various interoperability approaches.

We strongly support the ESB's policy direction, that new installations of CER should be 'flexible export ready'. However, we prefer the SA Power Networks proposal, which would:

- Distinguish between 'flexible exports ready' and 'flexible exports capable',
- Clearly define the terms 'flexible exports ready' and 'flexible exports capable',
- Mandate use of 'flexible exports capable' inverters nationally, and
- Allow DNSPs to determine the timing for the introduction of 'flexible exports ready' requirements in their own network.

It is crucial to ensure that the way that interoperability policy is implemented does not put customer choice at risk. The aim should be on open interoperability at all levels - devices and cloud platforms.

The ESB Directions Paper outlines the three models (native to the inverter, via a gateway device or via a cloud platform) and proposes that to comply with the mandate "at least one part of the technology model needs a compliant CSIP-Aus Client". However, there is a risk that in order to capture this cloud part of the data value stack, that OEMs will only provide access to a cloud CSIP-Aus client and device level interoperability will be lost. This would be the opposite of open interoperability. Even if a compliant CSIP cloud platform or CSIP gateway is available, every inverter should be required to have a minimum open communications protocol requirement - either SunSpec Modbus or IEEE 2030.5. What is important is that there is a minimum interoperability standard at the lowest level (the device level) which provides interoperability with the utility server without impeding device-to-device interoperability that customers will need for a home energy management system (HEMS) and other functions. This would not stop the use of CSIP gateways or a CSIP cloud platform, but it would protect consumers.

The Directions paper does not give adequate consideration to the role of metering coordinators and the benefits of an improved access framework for smart meter data. This is a significant omission.

There is no regulator that is well suited to regulating CER technical standards. The Clean Energy Regulator considers itself as a financial regulator. The Australian Energy Regulator (AER) is not a technical regulator. Technical regulators exist at the jurisdictional level (most notably, the Office of the Technical Regulator (OTR) in South Australia (SA), but a national approach to technical regulation is needed. We support the establishment of a National Technical Regulator, with responsibility for technical regulation of CER.

We strongly advise the ESB to avoid making recommendations regarding governance of CER technical standards that could appear to conflict with the direction proposed in the current Australian Energy Market Commission (AEMC) review of governance of CER technical standards.

In all of its policy development, the ESB should seek to regulate what entities are required to do and, as much as possible, refrain from stipulating how they should meet their regulatory obligations.

In our submission, we begin by outlining our key recommendations and the rationale for them, followed by detailed responses to the questions raised in the Directions Paper.

These issues are elaborated upon in our submission and we also provide responses to your specific questions. I remain available for further discussions and inputs.

Best regards,

Andrew Mears, PhD
Chief Executive Officer

T +61 421131550
E andrew.mears@switchdin.com

Key Recommendations

1. ***The metering provider should be included in the CER interoperability domains***

Access to smart meter data will be crucial to enabling better CER integration and interoperability.

2. ***The ESB should await the draft (if not the final) recommendations of the AEMC review of governance of CER technical standards before it proceeds further with development of interoperability policy and regulations***

It is crucial that the current confusion regarding roles and responsibilities for CER technical standards is clarified prior to the detailed design of the regulatory framework for CER technical standards.

3. ***The highest priority domain is CER to network. Following the implementation of dynamic operating envelopes and remote disconnection and reconnection, the most urgent and important use case for interoperability should be to improve compliance of CER with DNSPs' connection agreements.***

Policies cannot achieve its objectives without effective compliance and enforcement. Interoperability will enable remote digital verification of compliance.

4. ***Inverters should be required to have a minimum communications protocol requirement, even if a CSIP cloud platform or a CSIP gateway is available. CSIP-Aus should not be mandated as the only protocol allowed for CER-CER interoperability.***

To enable consumer choice, open interoperability is required at the device level, even if a CSIP cloud platform or CSIP gateway is available. However, CSIP-Aus has limitations at the device level and other open standards and protocols for interoperability should be permitted.

5. ***DNSPs will be best placed to enforce technical standards via connection agreements once the AEMC review has clarified and, if necessary, strengthened DNSPs' enforcement powers with respect to CER technical standards.***

The AEMC review of CER technical standards should provide the foundation for development of sound policy and regulation, supported by effective enforcement.

6. ***Policy makers should focus on what capability is required using internet connectivity. They should refrain from stipulating how to use internet connectivity.***

In all of its policy development, the ESB should spell out what companies are required to do and, as much as possible, should refrain from spelling out and mandating a solution.

7. ***We strongly advise against regulation by reference to a Standards Australia handbook.***

This would be the antithesis of best practice regulation.

8. ***A National Technical Regulator should be established to regulate CER technology, including the oversight of a national certificate authority and product certification and listing / delisting processes.***

Even if the AEMC commits to a process of annual review of technical standards, there will remain a need for day-to-day oversight of technical regulation. If a new regulatory authority is not established then the AER should fulfil the role of national technical regulator.

Responses to questions raised in the consultation paper

1. ***Are the five identified domains correctly summarised? Are there gaps or major limitations in the framing?***

There is a significant gap. Figure 5 omits the metering provider. The description of interlinkages with other workstreams (p.11) has omitted the AEMC review of metering services.

Access to smart meter data will be a crucial enabler of CER integration and utilisation of interoperability capability. Customers, or their authorised agents, should have a right to access near real-time data from the smart meter. This is needed to enable coordination of assets behind the meter. The customer pays for the smart meter, so they should have the right to access its data.

It would also be very helpful for DNSPs to have access to power quality data from smart meters so that they have better visibility of their low voltage networks and can use that data to calculate flexible export limits.

If Figure 5 is intended to represent an operational stakeholder model, then the definition of domains is unclear and appears to assume certain operational architectures which are arbitrary and inconsistent with subsequent discussions on interoperability models. Notably, domain 5 assumes that the CER Technology Providers participate in operation of the system which implies a certain system architecture. This is unclear due to the aggregation of several key stakeholders within the Technology Provider role and this leads to an undifferentiated treatment which obfuscates important considerations.

When considering interoperability for the use case of compliance and enforcement in the installation and commissioning phases, the domain in Figure 5 should be expanded to highlight the roles of the CER retailer, CER installer and CER OEMs, as outlined in Figure 2 of the Directions Paper. Explicitly including the CER retailer in the domain for the compliance and enforcement use case is important because they should have responsibility for providing the DNSP with evidence that the system they arranged to connect to the network was installed and commissioned in a compliant manner, satisfying all technical standards as required by the NER and the DNSPs connection agreement. The technology to enable remote verification of compliance with connection agreements is available but the regulatory framework does not support this. The AEMC is clear that the DNSP is the responsible party for determining whether CER complies with the technical standards via the connection agreements. The connection agreement establishes obligations of the consumer to the DNSP, but does not enable DNSPs to take enforcement action against CER OEMs or installers. SwitchDin has recommended the AEMC review of CER technical standards should assess whether DNSPs have the tools at their disposal to discharge their obligations under the National Electricity Rules (NER) and, if not, to strengthen their enforcement powers. Resolving this issue of governance is a crucial first step.

Recommendation 1:

The metering provider should be included in the CER interoperability domains.

Recommendation 2:

The ESB should await the draft (if not the final) recommendations of the AEMC review of governance of CER technical standards before it proceeds further with development of interoperability policy and regulations.

2. ***What priority should each domain be assigned, considering the interest of all electricity consumers within the consumer energy resource interoperability landscape?***

The first use case for CSIP-Aus will be flexible export limits, which will be within the CER to network domain. The first version of CSIP-Aus was developed for this purpose and application at scale is scheduled to commence in South Australia (SA) from 2023.

We anticipate the second use case will be remote disconnection and reconnection (also known as the 'emergency backstop'), operating in the same domain and using the same systems and capabilities flexible export limits.

Looking beyond flexible export limits and remote disconnection and reconnection, we recommend the following policy principles to guide prioritisation of use cases:

1. Improve system security and network operation, initially through improved compliance with connection agreements,
2. Support better value for consumers by avoiding 'lock in' to a single CER technology provider and by ensuring direct device-to-device interoperability behind-the-meter,
3. Drive uptake and deliver broad market benefits by enabling market participation.

Based on this order of policy priorities, we recommend the following order of CER interoperability domain priorities:

1. CER to network,,
2. Behind-the-meter,
3. CER to market,
4. DNSP to X (noting that some use cases in this domain are more urgent and important than others)

The most urgent and important use case for interoperability should be to improve compliance of CER systems with DNSPs' connection agreements.

We are uncertain of the urgency of establishing interoperability between DNSPs and the Australian Energy Market Operator (AEMO), given that there are a small number of DNSPs and there are established channels for communication between AEMO and DNSPs.

Recommendation 3:

The highest priority domain is CER to network. Following the implementation of dynamic operating envelopes and remote disconnection and reconnection, the most urgent and important use case for interoperability should be to improve compliance of CER with DNSPs' connection agreements.

3. ***What are the likely costs and benefits for consumers associated with a national 'flexible export ready' mandate including in relation to future readiness of customer installations and installation costs.***

The costs and benefits for consumers of a 'flexible export ready' mandate will largely be determined by how 'flexible export ready' is defined and how the policy is framed, governed and implemented.

The most feasible and cost effective option for a national mandate is likely to be option 1 (p.28), which would require DNSPs to implement flexible exports using a utility server that supports the CSIP-Aus communications protocol. Option 2 (requiring DNSPs to ensure all new installations are 'flexible export ready') would not require a uniform national commencement date and could be implemented progressively by DNSPs when they are ready.

We support the SA Power Networks proposal, which would:

- Distinguish between 'flexible exports ready' and 'flexible exports capable',
- Clearly define the terms 'flexible exports ready' and 'flexible exports capable',
- Mandate use of 'flexible exports capable' inverters nationally, and
- Allow DNSPs to determine the timing for the introduction of 'flexible exports ready' requirements in their own network.

Under this model, a 'flexible exports capable' mandate would require all inverters to be capable of supporting an open interoperability communication protocol, but the site controller, client, export monitoring device and internet connection do not need to be present. A 'flexible export ready' mandate would be implemented when the DNSP is ready to support it and would require:

- 'Flexible export capable ' inverters,
- A CSIP-Aus software client and site control,
- An export monitoring device,
- An internet connection, and
- Registration with the DNSP's utility server, which would use the CSIP-Aus communication protocol.

This staged approach would result in significant cost savings to customers whose DNSP is not yet ready to support a 'flexible export ready' mandate.

We are concerned that the ESB is framing its policy in terms of CER technology architectures. Framing the policy in this way lends itself to requirements enforcing commercial advantage of some Technology Providers over others. This framing could inadvertently lead to locking in certain technology solutions (e.g. by making an application programming interface (API) at the cloud level the only interoperability option) while locking out other technology options and thereby limiting customer choice and reducing effectiveness for some applications. .

There should be an obligation on CER Technology Providers to ensure that the relevant fleet of CER systems responds as required to instructions from the DNSP and that there is data available to verify compliance. In other words, the NER should specify what capability must be available from customers' systems. The DNSP's connection agreement should specify what capability must be implemented.

The DNSP's connection agreement should not limit device-levels options to CSIP-Aus only. Even if a CSIP-Aus cloud platform or CSIP-Aus gateway client is available, every inverter should be required to have a minimum communications protocol requirement, such as SunSpec Modbus, IEEE 2030.5 or the Open Charge Point Protocol (OCPP) for electric vehicle supply equipment (EVSE). What is important is that there is a minimum interoperability standard at the lowest level (the device level) and that this should provide interoperability with the utility server but not impeded device-to-device interoperability that customers will need for a home energy management system (HEMS) and other functions. For example, in California Rule 21 there are multiple options available at the device level being DNP3, SunSpec Modbus and IEEE 2030.5 and at least one of these must be available on the device even if there is a CSIP cloud service. This would not stop the use of CSIP gateways or a CSIP cloud platform, but it would protect consumers.

Limitations of CSIP-Aus at the device level

The Directions Paper (p.12) uses the example of TCP/IP, which is an interoperability standard for devices. It is used in the cloud because cloud is made up of devices. This is a poor choice of example because the communications protocols we require for interoperability are at a higher level than is supported by the TCP/IP stack. Using a CSIP cloud negates all the advantages of the TCP/IP protocol as it undermines the potential for device-to-device, which TCP/IP was designed to enable.

An Analogy

There is a good analogy with smart phones. At the moment if you want to play music on your APPLE iPhone you fire up the SPOTIFY app and it plays music buffered from the SPOTIFY cloud service by directly communicating with the SPOTIFY service via the internet without going through the APPLE cloud. Imagine if all the apps on your iPhone had to go through the APPLE cloud API rather than directly to the app service. It could work, but APPLE would add no value and they would just monetise the data pathway and add unnecessary costs to the user. This approach was actually tried in the early days of mobile smart phones as manufacturers started to build different app stores models, however it proved difficult to scale and customer choice was limited to only those apps that integrated with that phone OEM.

When it comes to device level interoperability, we can extend this smart phone analogy. Say you want to play music from the SPOTIFY app running on your iPhone to your BOSE wifi speakers. At the moment you just fire up the SPOTIFY app which has buffered your music on your iPhone and then your iPhone talks directly to your BOSE speakers via your home wifi network to play the buffered music. Imagine if you first had to make sure SPOTIFY and BOSE had an integration with APPLE. Then your iPhone would need to tell the SPOTIFY cloud service via the APPLE cloud API to send your music to your specific BOSE speaker via the internet. To do this, the SPOTIFY cloud would need to talk with the BOSE cloud. This could work, but it would mean that one of these parties (could be APPLE, SPOTIFY or BOSE) would need to know everything about your devices and how you need these devices to interact. This approach ignores the device level interoperability of the internet (e.g., TCP/IP)

Recommendation 4:

Inverters should be required to have a minimum communications protocol requirement, even if a CSIP cloud platform or a CSIP gateway is available. CSIP-Aus should not be mandated as the only protocol allowed for CER-CER interoperability.

4. ***Do stakeholders agree that DNSPs are best placed to enforce a 'flexible export ready' mandate at the time of installation? If not, what alternative models should be considered?***

The AEMC review of governance of CER technical standards is the best place to review the roles and responsibilities of DNSPs and other parties in relation to mandates enforced as part of the connection agreement. We acknowledge that the direction paper states, "This paper will highlight roles and responsibility issues raised in the specific context of interoperability that will be investigated more fully through the AEMC CER Technical Standards Review process" (p.10). We urge the ESB to provide its views on roles and responsibilities to the AEMC for consolidation into a single position. It could be very unhelpful for two market bodies in the NEM to undertake concurrent reviews of roles and responsibilities for implementation and compliance with CER technical standards, especially if the views of the AEMC and ESB are not aligned.

The AEMC is clear[1] that the DNSP is the responsible party for determining whether CER complies with technical standards via the connection arrangements. The challenge for DNSPs is that the current regulatory framework hinges on the connection agreement, which is between the DNSP and the

[1] https://www.aemc.gov.au/sites/default/files/2022-09/220928_emo0045_consultation_paper_-_public_version.pdf, p.24

customer. This leaves the DNSP with the unusable enforcement option of disconnecting the customer due to non-compliance by the installer.

If DNSPs are given responsibility for enforcement, they will need enforcement tools. This could include:

- Arrangements for data exchange between DNSPs and the Clean Energy Regulator regarding compliance rates observed for individual installers,
- Clarifying whether DNSPs can require CER retailers to provide data to verify compliance of their fleet of CER systems with the DNSP's connection agreements, and
- Clarifying whether DNSPs have the power to refuse connection agreements with installers who have a track record of persistent non-compliance.

Alternatively, the roles of the CER retailer, CER OEM, and CER installer could be defined in the NER. This would enable the Australian Energy Regulator (AER) to regulate CER installers, retailers and OEMs directly, rather than indirectly via DNSPs.

Recommendation 5:

DNSPs will be best placed to enforce technical standards via connection agreements once the AEMC review has clarified and, if necessary, strengthened DNSPs' enforcement powers with respect to CER technical standards.

5. ***What requirements should a flexible export ready installation have with regard to internet connectivity (e.g. embedded mobile communication versus LAN connectivity)?***

This question is an example of what the ESB should not do. There are pros and cons of embedded mobile communication versus LAN connectivity. The ESB should refrain from telling industry how to fulfil its obligations. Policy makers and regulators should spell out requirements and not the solution. For example, we should expect a certain level of availability e.g. 95%. This number doesn't need to be as high as for large scale regulated assets as the service is ultimately aggregated. However, it should not be so low as to undermine the whole business case for CER flexibility.

With respect to compliance requirements, consumers should not be exposed to additional costs unless this is done very transparently. For example, if using the customer's internet, regulators should aim to limit data consumed for the purpose of compliance.

Recommendation 6:

Policy makers should focus on what capability is required using internet connectivity. They should refrain from stipulating how to use internet connectivity.

6. ***What are the pros and cons of a 'flexible export ready' mandate set in the Rules, via a subordinate instrument or under a separate head of power (e.g. jurisdictional technical regulation)?***

A national (or NEM-wide) approach is strongly preferred to regulations that vary by jurisdiction and connection agreements that vary by DNSP. A uniform approach reduces costs to OEMs and DNSPs, and ultimately leads to lower costs for all consumers.

If technical standards are set in the NER, there is a very high risk that technology will be held back because regulatory reform is unable to keep pace. There would be a need for a fast, flexible and transparent standards setting process.

A faster and more flexible process would be for the NER to refer to a new standard that focuses on interoperability of devices or, alternatively, a new section of the AS 4777.2 standard. Regulation by

reference to standards has the risk of inadequate transparency and insufficient regard to regulatory impact assessment. If CER is regulated by references in the NER to Australian Standards, it should become the responsibility of the AEMC to ensure that there is sufficient consultation, cost-benefit analysis and business impact assessment to meet Australian Government expectations of best practice regulation.

7. ***If implemented under the Rules, which market body is best placed to establish and oversee the proposed requirement on DNSPs?***

If implemented under the Rules, then the AEMC would be best placed to make the new Rules and the Australian Energy Regulator (AER) would be best placed to oversee them. The AER is not currently fulfilling the role of Australia's national technical regulator for customer energy resources. There might be a need to formalise this as a new role for the AER and develop new expertise.

Alternatively, the Federal Parliament could legislate to create a new National Technical Regulator.

8. ***What are the pros and cons of a flexible export ready mandate referring to CSIP-Aus in Standards Australia handbook form?***

It would be very poor regulatory practice if the Australian Common Smart Inverter Profile (CSIP-Aus) were to be mandated by reference to a Standards Australia handbook.

It would be preferable to adopt the contents of the Standards Australia handbook as either a new section of the AS 4777.2 standard, or as a new standard focused on interoperability. This would ensure a higher level of rigour and more detailed consideration of testing procedures. Even if contents of the handbook are adopted as a new Australian standard (or as part of the existing AS 4777.2 standard), the AEMC should be responsible for ensuring there is an adequate process of consultation and Regulatory Impact Assessment, including cost-benefit analysis. Regulations that refer to a Standards Australia handbook would, in effect, give a Standards Australia committee the power to amend regulations without the normal checks and balances of best practice regulation.

Recommendation 7:

We strongly advise against regulation by reference to a Standards Australia handbook.

9. ***Would there be value in agreeing a national approach to public key infrastructure for consumer energy resources?***

Yes. Public key infrastructure will be important to ensure data security. Multiple approaches by different jurisdictions would be inefficient and would add unnecessary costs.

10. ***Are there existing examples that could be used as a model for the consumer energy resources ecosystem?***

There are no comparable CER markets overseas that are comparable or more advanced than Australia with respect to CER interoperability and upon whom we could model or approach to regulation of flexible export capability.

The situation in the USA especially in California where the California Rule 21 provided a mandated device-level requirement (CER-DNSP+Trader) for devices to provide minimum communications capabilities is at a much earlier stage and does not address the key use-cases or the disaggregated market structure of Australia. It is important to note that this rule mandates not one protocol only, but allows one of three possible protocols, namely DNP3, Sunspec or IEEE 2030.5. Subsequent discussions of CSIP via cloud API have raised serious concerns around risk of limiting customer

choice and increasing costs, and cyber-security risks and management overheads of relying on unregulated OEM cloud infrastructure.

There are also limitations with CSIP-Aus which would bring into question any decision to mandate it. Those limitations include:

- There are no proper test and certification capabilities for CSIP-Aus,
- The effectiveness and efficiency of CSIP-Aus at scale is unproven as there are no at-scale aggregations using either CSIP or CSIP-Aus,
- Utilising CSIP-Aus at the cloud may require DNSPs, aggregators, and traders to utilise the OEM clouds over which they do not control end to end cyber-security,
- The at-scale cyber-security and sovereign data risks are unquantified for CER in general and reliance on OEM cloud platforms exacerbates these uncertainties, and
- The reliance of CSIP and CSIP-Aus on specific "utility handbooks" which guide Technology Providers in the compliance requirements of specific DNSPs would mean that if even CSIP-Aus were adopted by all DNSPs, 'rail gauge' issues would still arise.

11. What are the pros and cons of establishing a national certificate authority?

The advantages of a national authority would include:

- Better for security,
- Better for privacy,
- Lower costs for industry and consumers,
- Improves ability to manage the specific requirements of CSIP-Aus compliance, and
- Root certificates would be Australia-based, aligning with Australian critical infrastructure requirements.

The main disadvantage would be that there does not appear to be a national body that is well placed to take on the role. Establishing a new body could be time consuming and resource intensive.

12. Do stakeholders have a view as to who should perform the role of national certificate authority, if it were created?

If there were a national technical regulator for CER in the NEM, it would be well placed to perform the role of national certificate authority, possibly working in collaboration with the Australian Cyber Security Centre or the Australian Signals Directorate. The administration could be outsourced to a key industry body but there would be a need for oversight by a regulator with technical expertise.

13. What views do stakeholders have about the adaptability of existing industry-led product certification and compliance processes for future use?

The existing industry-led product certification and compliance processes rely upon eligibility for the Small-scale Renewable Energy Scheme (SRES) as the key driver to encourage compliance by OEMs. The value of the solar rebate available under the SRES scheme is scheduled to wind down each year, reaching zero by 2030. It is anticipated that prior to 2030 the cost of meeting SRES eligibility requirements could exceed the benefits available in the form of rebates. At that stage, the current product certification and compliance processes will no longer be fit for purpose.

The compliance regime for CER installers and OEMs needs to transition from a scheme underpinned by incentives to a scheme underpinned by regulation and this needs to occur within the next few years and no later than 2030. SwitchDin has recommended the AEMC review of governance of CER technical standards consider strengthening the compliance regime, either by clarifying and, if necessary, strengthening the enforcement powers of DNSPs with respect to CER retailers, or by

amending the NER so that CER OEMs, CER retailers and CER installers can be regulated directly, rather than indirectly via the DNSP. It is also worth noting that the Clean Energy Regulator is considering changes to the administration of industry-led product certification and compliance schemes under the SRES.

To avoid unnecessary confusion, we recommend awaiting the draft report (if not the final report) of the AEMC review of governance of CER technical standards and the Clean Energy Regulator review of the product compliance scheme under the SRES prior to making recommendations regarding potential changes to the governance and operation of industry-led processes.

14. ***What views do stakeholders have about the most appropriate body to have oversight of the product certification and listing / delisting processes?***

CER products should be tested by accredited third party test labs to an approved test procedure that is part of an Australian or international standard. A register of compliant products should be administered by a national body such as the CEC. The administration function should be overseen by a regulator with sufficient technical expertise for the role.

There is no regulator that is well suited to regulating CER technical standards at the device or cloud level. The Clean Energy Regulator considers itself as a financial regulator. The AER is not a technical regulator. Technical regulators exist at the jurisdictional level (most notably, the OTR in SA), but a national approach to technical regulation is needed.

We support the establishment of a National Technical Regulator, with responsibility for technical regulation of CER. If established, the National technical Regulator would be the most appropriate body to have oversight of product certification and listing / delisting processes.

Recommendation 8:

A National Technical Regulator should be established to regulate CER technology, including the oversight of a national certificate authority and product certification and listing / delisting processes.

15. ***What role could DNSPs have in the product certification / decertification process in the context of improving outcomes for industry and consumers?***

This should be determined through the AEMC review of the governance of CER technical standards.

DNSPs should operate within a regulatory framework that clearly specifies what they can expect from whom, and what actions they can take in response to non-compliance. For example, the NER should answer questions such as:

- Can the DNSP require CER retailers to provide evidence of compliance of CER with technical standards as required by the NER and connection agreements?
- What enforcement powers are available to a DNSP in relation to compliance with requirements of the NER and connection agreements?

SA Power Networks has taken a leading role in the establishment of a CSIP-Aus compliant utility server and using it to verify compliance of CER with its 'flexible export ready' requirements. While this has been a helpful contribution, it would be unhelpful for every DNSP to develop its own unique procedure for verification of 'flexible export ready' compliance of CER. The work that has been led by SA Power Networks should transition to a framework for verification according to a replicable test procedure.

In the circumstances, it made sense for SA Power Networks to develop its own testing and certification procedure. In the longer term, DNSPs should not be responsible for product certification / decertification processes. The DNSPs' focus should be on the entities with whom they have

arrangements, not the products managed by those entities. There should be a standardised test procedure used by all DNSPs or other organisations required to verify compliance with ‘flexible export ready’ requirements.