



7 March 2025

SwitchDin Pty Ltd

Department of Climate Change, Energy,
the Environment and Water (DCCEEW)

ACN 154 893 857

Response to Questions in Consultation Paper: *NSW Emergency Backstop Mechanism and Consumer Energy Resources Installer Portal*

Thank you for the opportunity to provide a response to DCCEEW's questions regarding the NSW Emergency Backstop Mechanism & CER Installer portal..

SwitchDin is a technology provider helping participants in the energy sector make the transition to renewable energy. We provide systems and solutions to give visibility and control of distributed energy resources, including consumer energy resources (CER). In this role we have a keen interest in the connection process so that consumers can more easily, efficiently, and effectively use these resources in ways that benefit not just themselves, but also the grid as a whole. We are especially concerned to ensure that consumers can recover good value from their investment in CER and that the CER can participate effectively when connected to the energy grid.

Please find below our responses to the questions raised in the Consultation Paper.

Sincerely,

SwitchDin

1. Do you support the requirement for NSW DNSPs to harmonise their implementation of the backstop mechanism?

Yes, experience in other jurisdictions has shown that reducing inconsistencies and differentiation between networks is a key contributor to an efficient and workable solution for emergency backstop. It also provides a foundation for other features that will benefit CER consumers.

2. Are the scope and timelines for the emergency backstop mechanism feasible?

There is a need to maintain urgency and ensure a timely implementation. Spring 2025 presents a genuine challenge for network stability that should be considered.

However, it would be counter-productive to rush the implementation of a system that would be ineffective and a hard deadline for the full functionality might force implementors to cut corners and render the system ineffective, even on day one. There is some evidence that implementation efforts in other jurisdictions have suffered this fate.

We suggest that the relevant players (especially the NSW Government and the DNSPs, working with their suppliers) should cooperate on a “minimum viable product” (MVP) that would be achievable in the Spring 2025 timeframe. Best efforts should be made to achieve this MVP goal.

The MVP could include:

- An agreed and consistent mechanism for the emergency backstop mechanism to be implemented across all DNSPs, including consistent expectations of behaviour from CSIP-AUS controlled devices.
- A single process for CER device suppliers (OEMs) to obtain device type certification for their equipment to connect to *all* DNSPs, with a reliable pathway to obtain authority to connect by testing with *any* DNSP.
- A consistent installation and connection process, supported by DNSP and/or government portals, that allowed installers to reliably install CER devices. This initial version may have inefficiencies, but it should be reliable.

- Consistent reporting of the total power available for backstop control across each DNSP, with an agreed level of quality and frequency for this data.

Ongoing milestone targets beyond the MVP should be established. These should continue to monitor both key capabilities being developed and the total amount of backstop capability reliably available for the emergency backstop mechanism. Ongoing efforts, with greater accountability, should be made to achieve these targets.

3. Do you agree with the order of the hierarchy of measures to increase operational load in the grid during MSL events?

The proposed hierarchy of measures is good. It aims to ensure that all other avenues to increase system load are attempted before curtailing consumer export or, more stringently, generation.

While there is a compelling need for an emergency backstop measure, the focus on implementing this runs the risk that other, more consumer-friendly, measures will be deprioritised. Alongside the activity to get an effective emergency response, there should be ongoing work to provide other incentives (including commercial incentives) to allow consumers' solar PV energy to be used rather than curtailed. As these measures are developed, their capabilities and effectiveness should be included in the planning and forecasts for future backstop capacity requirements.

4. Are the design elements of the backstop mechanisms appropriate and feasible?

The five proposed design elements are appropriate, with the following caveat.

For the Communication network (*item 3*), most CER devices rely on consumer internet connections, which will be somewhat unreliable. But enforcing a truly reliable communication backup may be very expensive. Using the consumer's network may be sufficient with ongoing monitoring of connection and actions taken to notify & rectify when it's out for an extended period. The "Local Fall-back behaviours" can encompass this, but it may also need modifications to customer

connection agreements (*item 5*) to make customers aware of any ongoing responsibilities.

We believe that a mechanism based on CSIP-AUS is consistent with the suggested design elements, additionally, alongside the listed elements reliable and consistent Public Key Infrastructure (PKI) should be used to secure device and server identity, and this should be aligned with efforts already underway to establish a nationally consistent PKI for energy systems. In particular there should be a single root CA for NSW to make future migration to the national PKI simpler.

5. Are the roles and responsibilities of each organisation appropriate and feasible?

As a list of responsible parties, the proposed list is reasonable, with some minor modifications.

Point 1: The Original Equipment Manufacturers (OEMs) of CER are responsible for developing the device functionality (e.g. CSIP-AUS protocol compliance, PKI registration, etc.). Installers will be responsible for configuring the devices to correctly use that functionality (e.g. ensure the correct PKI certificates are used, configuring the CSIP-AUS client, etc)

Point 5: Energy retailers need to be involved in contractual agreements with customers (and any ongoing customer communications required).

6. Do you support the threshold for backstop mechanism using CSIP-AUS being 200kW and smaller?

CSIP-AUS is well suited for systems less than 200kW, and is used that way in other parts of the country. Working towards national consistency by aligning with other states is beneficial.

I. Do you agree with the approach for systems above 200kW? If not, please explain why and provide any alternative suggestions.

Using CSIP-AUS for larger systems also has benefits including:

- A. Enabling data about all CER to be collected with a single consistent mechanism
- B. Being more cost effective than traditional systems based on SCADA
- C. Easier inclusion of the growing number of EV charging sites that will operate above 200kW

On point A, for instance, it will be significantly easier to calculate the total capacity that is available for reduction under emergency backstop conditions if all participating sites use CSIP-AUS to report on their status.

7. Do you have any concerns or insights into using CSIP-AUS compatible inverters and an internet connection to control the backstop mechanism?

CSIP-AUS is the right protocol to drive national consistency for connection of CER. It has been used by other DNSPs in Australia for a number of years for their Emergency Backstop and/or Flexible Exports programs and being nationally consistent has many benefits.

CSIP-AUS can also be used for other important use cases, including flexible exports, dynamic network pricing, and fully dynamic connections with both flexible import & export limits. For example SAPN has used CSIP-AUS to enable them to reliably run their network with >100% of instantaneous operational demand supplied from rooftop PV. Making these use cases available via a nationally supported standard will provide much better choice and value for consumers rather than following a myriad of proprietary, device-dependent protocols.

Enabling control over internet connections (which is generally how CSIP-AUS is implemented) is a practical and cost-effective approach. As consumers rely heavily on the internet for daily life, the connections themselves are becoming more robust and reliable. There are still cases, however, where devices may lose connectivity to the local network (e.g. when a home wi-fi password is changed)

and therefore be excluded from CSIP-AUS control mechanisms. Procedures for dealing with this should be enhanced, including:

- a. Ensuring the connection agreements include obligations on the system owner to maintain the internet connection to CER devices,
- b. Providing incentives to ensure that the connections are properly maintained (e.g. falling back to lower export limits if connectivity fails for an extended period and/or enabling a bill discount when connection is maintained), and
- c. Ongoing monitoring of the status of CER device connections and having procedures in place for remediation, including communications with the device owner.

8. Is it appropriate for the emergency backstop mechanism to be implemented using technologies and systems consistent with enabling the future use of flexible export limits?

Yes, and it's desirable, as this approach minimises costs, and accelerates the availability of these important use cases that foster greater consumer benefits, and reduce the chance the Emergency Backstop system will need to be activated.

Aligning the backstop implementation with future use cases should be the intention from the start, not an optional extra.

Having a nationally consistent approach is an important factor in the success of these future use cases, and the backstop implementation should work towards achieving alignment between NSW and other jurisdictions.

9. Which, if any, existing test protocols should be considered for implementation as the consistent test protocol for NSW?

It is important to draw a distinction between "device type testing" (performed by an OEM as part of gaining approval to generally be able to connect a device / model to the grid) from "commissioning testing" (performed at installation time to confirm the specific devices at a site have been correctly configured).

The device type testing should be managed with "authority to connect" for a device type from each DNSP. Ideally this will be consistent for all DNSPs (i.e. one test

should give authority to connect to all DNSPs). The list of approved devices should be maintained on an ongoing basis (e.g. updated for each new release of equipment and re-tested periodically, or on key changes like model software revisions). As this process is a burden the OEMs must bear to sell their equipment, the process should be made as easy as possible for them to minimise costs they have no avenue to recover other than via consumer pricing. This suggestion is similar to the approach taken in South Australia, where a development & integration testing server is available to OEMs, and the type testing is performed against this central system.

On-site commissioning testing at installation time should be performed via the installer portal, and the testing process should be part of connecting to the relevant DNSP's live CSIP-AUS environments.

10. Do you think the conditions under which the emergency backstop mechanism could be used are appropriate?

The proposed trigger conditions for the backstop mechanism are appropriate. It's important that all other actions have been exhausted before activating the backstop mechanism. This will ensure that curtailing solar generation only occurs in rare circumstances, as needed to ensure system security is maintained.

Experience from other jurisdictions shows that having public buy-in is critical for the widespread adoption of these backstop systems. We suggest emphasising to participants (including consumers) that this mechanism is part of a broader strategy to allow more exporting/sharing of solar power that is being executed across the industry. The backstop mechanisms are an essential guardrail to enable that.

There will also be greater buy-in if there is sufficient transparency & oversight to ensure this system is only used as intended, and consumers are empowered to review the actual impacts the backstop has had on them (which are expected to be minimal). Having requirements to publish data about activations of the Emergency Backstop system (including for testing purposes) will enable that.

11. Do you have any views on the proposed implementation pathway (variation of DNSP licencing conditions) or alternatives??

Varying the DNSP licence conditions is a pragmatic way to enforce action and enable a rapid implementation.

12. What information will manufacturers, installers, customers and distribution networks require to understand the changes to implement the backstop mechanism?

Different audiences need different information, however there first needs to be coordination and alignment between the DNSPs to enable interoperability. For instance, the network connection requirements must be aligned across DNSPs before a unified mechanism for OEMs to get authority to connect is possible (see response to question 9).

All parties integrating with the systems (e.g. DNSPs, and OEMs) will need complete technical specifications, users of the system (e.g. installers & DNSPs) will need documentation & training, and end consumers should have access to information to help them understand how the backstop mechanisms relates to them.

There are other stakeholders such as electricity retailers that will be impacted, and would benefit from access to information.

i. Who is best placed to communicate this information to the different audiences?

Communication will need to be coordinated among many industry participants. The NSW state government is well placed to play a role in coordinating the communication processes to ensure consistency. It can also facilitate the public education needed to avoid the negative perceptions that have arisen around Emergency Backstop Measures in other states

Communication should leverage existing relationships. DNSPs and OEMs may already have good communications channels to installers. Retailers & installers

both have relationships with end customers. All of these relationships should be exploited to communicate necessary information.

ii. How should this information be best communicated to the different audiences?

Beyond leveraging the existing relationships to communicate initial changes, best practice will be to ensure that good communication is built into the routine processes that are used to implement the mechanisms. For example, when OEMs want to connect a new device, they should be referred to a single, consistent, well-described source of information that covers device type approval for all DNSPs. When installers need to connect individual devices, the same consistency should be maintained, including the clear and consistent communication through the Installer Portal.

13. What CER should the NSW CER Installer Portal capture?

I. What types of technology?

Any CER connected with CSIP-AUS (or, in future, any other protocol that is adopted as the standard for control of DER) should be covered by the portal to ensure consistent trustworthy data.

II. What size (capacity) of technology?

Any capacity covered under the adoption of CSIP-AUS.

III. What technology should be excluded? Why?

No exclusions – the CER installer portal can provide a consistent entrypoint for reliable data about all installed CER. However there must be enough fidelity in the processes and data to accurately determine what is connected, and which programs those devices should participate in. (As an example, batteries are a useful tool to increase load on the network, so they should not be inadvertently disconnected by incorrectly associating them with the Emergency Backstop disconnect mechanism.)

IV. Should the Portal align with the Emergency Backstop Mechanism in capturing only systems under 200kW?

This restriction does not seem to be beneficial if the goal is to ensure consistent and reliable data is recorded about all CER in AEMO's DER Register.

V. Should the Portal capture technology consistent with that recorded in AEMO's DER register? Is there additional technology that should be captured?

Yes. The portal should be used to improve the validity and coverage of the DER register. If the DER register needs to be expanded for additional technology controlled by CSIP-AUS, it should be, so that there is a consistent approach to managing DER.

Both the existing DER and any future extensions should consider personal information that might be held and protect it carefully. Clear ownership of the data should be established, including the rights of consumers who own the DER equipment to access and control data for their DER appropriately.

14. Do you support the functions outlined for inclusion in the CER Installer Portal?

We agree with the Portal functionality as outlined, with the clarification that as described, the Portal "compliance" test is checking for compliance of the device as it is installed at a site. It will be doing a "commissioning acceptance test" of key functions to ensure that installation has been done effectively.

Prior to any device being installed, it should have passed a more extensive "device type acceptance test" for that brand and model of device. This is done today for devices on the Clean Energy Council (CEC) "white list" of inverters, relied on by SAPN for their SmartInstall process, but the NSW Emergency Backstop mechanism should ensure that this test regime and list is maintained on an ongoing basis.

The *device type acceptance testing* should not be done through the Portal, but should be a pre-requisite for devices of that type to be available on the Portal.

15. Are there any additional functions you would like to see included within a CER Installer Portal?

No. It's good that the Portal is updating the AEMO DER Register for a new installation. One of the problems with the latter is that there is no effective mechanism to keep the Register accurate. A process to maintain the accuracy of the data in the DER Register is required, but it is beyond the scope for the Installer Portal.

16. Are there additional ways that the Portal should be designed to support installers?

Two problems occurred for installers in Victoria:

a. When failure occurred in the installation process, it was not clear to the installer what the cause of the failure was and what was required to remedy it. So, if problems arise during the installation process, the Portal should be designed to make it easy for installers to know what the next steps are to remedy the problem (including what support might be required and/or technical documentation to assist with troubleshooting).

b. Some types of installation failed consistently, e.g. all attempts to install a certain device or all installation attempts in a certain area. So, the Portal could include anomaly analysis that would identify when multiple installation failures are occurring, so that these could be investigated.

If another goal of the installer portal is to enable high quality data entry, then opportunities to automate data capture should be explored with OEMs and DNSPs to minimise the need for installers to perform large amounts of manual data entry.

17. Do you agree that the party that applies for a CER connection should be responsible for ensuring the installers they have engaged rectify non-compliance?

It's not clear to us what is meant by "the party that applies for a CER connection" in this case. If the home/site owner is intended, we expect there may be many cases

where the application has been made by the installer on their behalf. In this case, the installer should be directly responsible to rectify any non-compliance issues prior to having the installation certified. If another party, other than the owner or installer, initiates the connection request, then it's reasonable for that party to be responsible to follow up with the installer. There should also be clear information available about the escalation paths in the case that an installer is uncooperative in rectifying issues.

18. Do you have any other views on compliance and enforcement within the Portal?

Nothing further to add. Previous responses have highlighted that a comprehensive approach to compliance needs ongoing assurance processes in addition to different styles of point-in-time testing.

19. See answer for Question 16

20. Do you agree with the phased approach proposed for the delivery of the Portal?

Yes. See Q2 for further details.

21. Do you think that there are any functions that should be included or excluded from the first phase of the Portal development?

"Device type acceptance testing", as outlined above, should not be a Portal function but should be a pre-requisite for inclusion in the Emergency Backstop Mechanism, even for the first phase.

22. Do you support the proposed joint NSW Government–DNSP delivery of the CER Installer Portal?

Yes, with the condition that alignment between DNSPs can be achieved, and the joint delivery includes processes to reduce the overall burden of implementation and adoption by OEMs and other impacted parties.

For example, the suggested approach is to build on the progress made by Endeavour Energy, so an OEM should be able to perform device type testing with Endeavour now and obtain an authority to connect which will be transferable to Ausgrid & Essential Energy’s networks in the future, without requiring OEMs to develop new clients or perform re-testing for previously approved device types.

23. What information will installers and any other stakeholders require to support the roll out of the CER Installer Portal?

Particular care should be taken to ensure that:

- OEMs have information about technical requirements & CSIP-AUS capabilities and how to obtain “device type” certification
- Installers know that the devices they are installing have been accepted for connection by all the DNSPs, and know how to go through the process of on-site CSIP-AUS configuration and commissioning testing when connecting CER
- The general public has enough information to understand the value of the Emergency Backstop Mechanism as a key enabler of the border consumer energy strategy

I. Who is best placed to provide this information?

DNSPs collectively should be responsible for providing the necessary information to OEMs and installers to certify and install CER devices on their networks.

II. What are the best ways of communicating this information to stakeholders?

The communication of this information should be built into the relevant process flows (i.e. device type certification information should be available throughout the testing and certification process, the installer portal should guide installers on what they need to know). See Q12 for further details.