Utility interconnection handbook

Technical Specification

Ausgrid / Endeavour Energy / Essential Energy / Evoenergy

May 2026

Version 1.1

Ausgrid Endeavour Energy Essential Energy evoenergy

Contents

1 INTRODUCTION

1.1 Purpose

This document includes technical information relevant to the use of CSIP-AUS in NSW and ACT to support emergency backstop requirements and flexible connections.

1.2 Context

Acting on advice from AEMO, the NSW and ACT Governments have committed to introduce emergency backstop measures for rooftop solar systems. These are capabilities that enable the output of solar systems to be temporarily restricted during emergencies, when this is necessary to manage the risk of blackouts.

To support the backstop capability, solar installations need to be capable of receiving and acting on signals communicated by the DNSP using CSIP-AUS, the Australian version of the Common Smart Inverter Profile (CSIP) for the IEEE 2030.5:2018 communications standard. As of April 2026, CSIP-AUS is codified in Standards Australia Technical Standard SA TS 5573 (formerly SA HB 218).

As well as enabling emergency backstops, CSIP-AUS is the technology that enables DNSPs to offer flexible export limits, which allow CER customers to export more energy to the grid than traditional fixed limits. In future, CSIP-AUS will also enable a range of new market services for customers that choose them.

1.3 Scope

This document has been jointly prepared by Ausgrid, Endeavour Energy, Essential Energy and Evoenergy.

The CSIP and CSIP-AUS refer to a utility interconnection handbook to provide additional detail that may be utility-specific. This document is the utility interconnection handbook for the NSW and ACT DNSPs. It provides information relevant to Original Equipment Manufacturers (OEMs), Aggregators and others with CSIP-AUS-compatible equipment or systems that will be deployed in NSW and the ACT and will need to communicate with DNSP CSIP-AUS Utility Servers.

2 DEFINITIONS, REFERENCES AND ABBREVIATIONS

Term	Definition
Aggregator	Cloud system representing multiple downstream DER as defined in CSIP-AUS, acts as the Software Communications Client for DER. Also used to refer to the commercial entity responsible for same.
ANU	Australian National University
AS/NZS 4777.2:2020	Inverter requirements standard

Term	Definition
CER	Customer Energy Resource. Another name for DER owned by the customer.
CSIP	Common Smart Inverter Profile
CSIP-AUS	Common Smart Inverter Profile – Australia, as defined in Standards Australia SA TS 5573 or any superseding standard
CSIP-AUS Explainer	A document published by the national DER Integration API Technical Working Group that provides supplementary information on how CSIP-AUS is to be interpreted and applied. See: CSIP-AUS Explainer.
CSIP-AUS product	A product that is required by a DNSP to support CSIP-AUS and to actively communicate with the DNSP's Utility Server. For the purpose of this document, a product that happens to be CSIP-AUS capable is not considered to be a 'CSIP-AUS product' if it is not being used as such, i.e. if its CSIP-AUS functions are not being used.
DER	Distributed Energy Resource: Rooftop solar systems, home batteries, smart appliances, etc – small-scale resources distributed among homes and businesses that all participate in and contribute to the electricity system.
Direct Device	Defined as Client in CSIP-AUS, where the communications software client is hosted for the individual DER and connects directly to the Utility Server
DNSP	Distribution Network Service Provider. For NSW this is either Ausgrid, Essential Energy or Endeavour Energy. For ACT it is Evoenergy.
ENA	Energy Networks Australia
End Device	The physical DER device at the premises that is controlled by the CSIP-AUS Software Communications Client, e.g. an inverter.
Gateway	On-site hardware providing communications and control functionality to DER on site acting as a Direct Device Client
IANA	Internet Assigned Numbers Authority
IEEE 2030.5:2018	IEEE standard for Smart Energy Profile Application Protocol
LFDI	Long Form Device Identifier
NMI	National Metering Identifier
OEM	Original Equipment Manufacturer
PEN	Private Enterprise Number, a unique identifier issued to a private enterprise by the IANA
Utility Server	Server entity as described in CSIP-AUS

Term	Definition
Software Communications Client	2030.5 client to receive commands and send measurements

3 CSIP-AUS

3.1 Overview

CSIP-AUS is developed and maintained by the DER Integration API Technical Working Group (DERIAPITWG), an industry-led national working group convened under the DER Interoperability Steering Committee (ISC), part of the Distributed Energy Integration Program (DEIP) established by the Australian Renewable Energy Agency (ARENA).

This document assumes familiarity with the technical details of the CSIP-AUS communications protocol. Further details of CSIP-AUS can be found in the CSIP-AUS Explainer document published by DEIP and by reference to the most recent version of CSIP-AUS published by Standards Australia.

Readers should familiarise themselves with the above documents, particularly the CSIP-AUS Explainer document, as this includes details on how the standard is to be interpreted and applied. Unless otherwise stated herein, NSW and ACT implementations of CSIP-AUS will conform to the interpretation in the Explainer document.

3.2 Site configurations

Figure 1 below illustrates the different communication models that are possible between the Utility Server and the DER End Device (e.g. solar inverter), depending on whether the CSIP-AUS Software Communications Client resides natively on the End Device, within a gateway device on site that controls the End Device, or within a cloud service that controls the device. In the latter two cases, the communication protocol between the gateway or cloud system and the End Device is not specified. Refer to the CSIP-AUS Explainer document for further details.

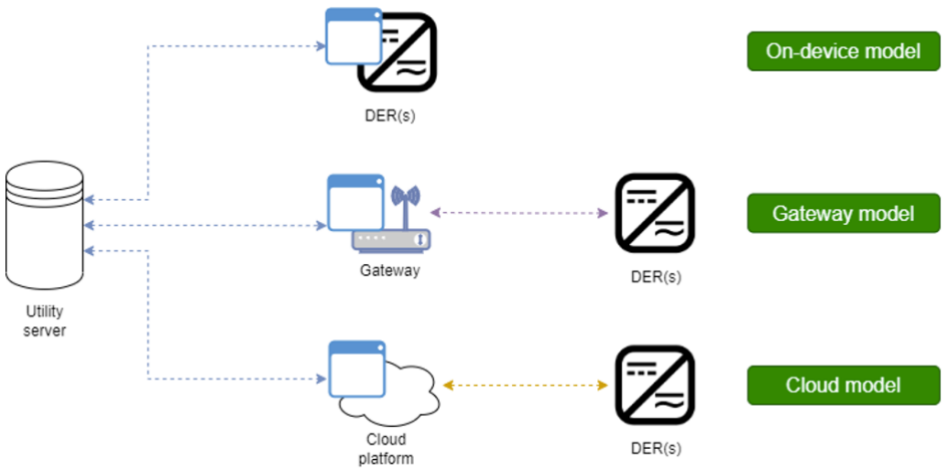

Figure 1 - CSIP-AUS site configurations

In all cases, the end-to-end configuration must ensure that:

- communications between the Utility Server and the Software Communications Client is via the internet and complies with IEEE 2030.5:2018
- the End Device behaves correctly according to the CSIP-AUS functional specification, including:
    - responding correctly to controls issued by the Utility Server
    - correctly reverting to required fallback behaviours (e.g. default export limits) if communication with the Utility Server is lost for any reason
- telemetry and control responses received by the Utility Server correctly reflects the current state of the End Device.

3.3 Utility Server environments

Each of the NSW and ACT DNSPs will operate its own Utility Server. Each DNSP will operate at least the following environments:

- a test Utility Server that OEMs and Aggregators can connect to during the onboarding process to confirm connectivity with the DNSP's network (see section 5)
- a production Utility Server that will communicate with CSIP-AUS products in the field.

The process for OEMs and Aggregators to request access to DNSP Utility Servers and to obtain the necessary digital certificates is described in section 5 below.

4 CERTIFICATION AND LISTING

4.1 Background

CSIP-AUS products to be installed in NSW and ACT must be listed by the Clean Energy Council (CEC) as compliant to the version of CSIP-AUS that was in force at the time of the DNSP approval to install the system.

Prior to November 2025, testing and certification against SA HB 218:2023 (CSIP-AUS v1.1) was performed by SA Power Networks on behalf of industry, and SA Power Networks was responsible for nominating products that had passed SA Power Networks' testing process for listing by the CEC as CSIP-AUS compliant. In cases where other DNSPs' implementations of the standard differed from SA Power Networks', OEMs and Aggregators had been required to conduct additional testing of their products against those DNSPs' individual utility servers.

A new version of CSIP-AUS was released in mid-2025. This version, SA TS 5573:2025 (CSIP-AUS v1.2), includes an expanded client test suite intended to provide a universal testing process that will cover all DNSP server implementations.

With the release of the new version of CSIP-AUS, a new national testing, certification and listing service has been established by the Australian National University (ANU) under the DEIP ISC. This new service launched in September 2025 and has replaced the SA Power Networks process as the means by which CSIP-AUS products are certified and listed with the CEC.

ANU has also developed a server testing tool based on the same reference implementation of CSIP-AUS that DNSPs can use to test their individual Utility Servers for conformance to the current version of the CSIP-AUS standard.

4.2 Certification and listing requirements for NSW and ACT

CSIP-AUS products to be installed in NSW and ACT must be listed by the Clean Energy Council (CEC) as compliant to the version of CSIP-AUS that is in force at the time of the application to install the system.

NSW and ACT DNSPs do not require OEMs or Aggregators to test and certify their products against their individual Utility Servers.

To ensure compatibility with products on the CEC list, NSW and ACT DNSPs intend to test their Utility Servers using the server testing tool being developed by ANU.

CSIP-AUS includes both mandatory and optional functions, and allows for DNSPs to prescribe how certain functions and behaviours are configured. These detailed requirements are set out in section 7 below.

As well as being certified as CSIP-AUS compliant as described above, a CSIP-AUS product may only be commissioned in NSW or ACT if the OEM or Aggregator responsible for the CSIP-AUS client has completed the onboarding process with the relevant DNSP, as described below, by the date on which the system is installed.

5 ONBOARDING

5.1 Overview

Onboarding is a once-off process that each OEM or Aggregator responsible for a CSIP-AUS client implementation must complete with each of the NSW and ACT DNSPs in order to be allowed to communicate with the DNSPs' Utility Servers.

Figure 2 – Onboarding process

The onboarding process is common across all NSW and ACT DNSPs. It is shown in Figure 2 above and summarised below. Further detail on specific steps in the process is included in the sections that follow.

1. Application

   The OEM or Aggregator must complete, as a minimum, Part A (company details) of the Utility Server Access Form included in Appendix A and submit the form to each DNSP that the OEM or Aggregator wishes to onboard with. An online form hosted by Ausgrid is available here and this will share the details with all NSW/ACT DNSPs.

   If an OEM or Aggregator does not wish to share details with all NSW/ACT DNSPs, forms may be submitted by email using the following email addresses:

   - Ausgrid: csip-aus@ausgrid.com.au
   - Essential Energy: csip-aus@essentialenergy.com.au
   - Endeavour Energy: csip-aus@endeavourenergy.com.au
   - Evoenergy: csip-aus@evoenergy.com.au

2. Preliminary approval

   Once an application has been received, and assuming the details provided in the application form are satisfactory, the DNSP will provide the applicant with the URL for its test Utility Server and arrange for a test certificate to be issued to the applicant that will enable client access to its test Utility Server.

   The DNSP will also engage with the applicant's nominated contact to agree on the process and timeframe for completing the remainder of the onboarding process.

3. Basic communication test

   The DNSP will coordinate with the applicant to perform a basic communication test to confirm that the applicant's CSIP-AUS client is able to communicate reliably with the DNSP's test Utility Server.

4. Full application

   The applicant must complete Part B of the Utility Server Access Form included in Appendix A. This includes declarations that the applicant has read, understood, and will abide by:

   - This Utility interconnection handbook, including the Guiding Principles for Utility Server Access in Appendix B

- The Common Cyber Security Requirements for DER.

These documents will be provided to the applicant during step 2, or are otherwise available on request by emailing one of the DNSPs using the email addresses above.

5. Approval and onboarding

   The above steps having been completed, the DNSP will enable client access to its production Utility Server. DNSPs may require another basic communication test with the DNSP's production Utility Server before the software client can be used.

5.2 Basic communication test

The intent of the basic communication test as part of the onboarding process is simply to confirm that the applicant's CSIP-AUS Software Communications Client is able to communicate reliably with the DNSP's Utility Server. It will not include testing of any product for compliance with CSIP-AUS functionality.

To ensure a smooth transition to production, it is in the applicant's interest to ensure that the client configuration and any associated software systems, services, firewalls and communications pathways used during the basic communication test with the test server match those that will be used in production.

5.3 Cyber security

Applicants must declare that they have read, understand and will abide by the requirements in the Common Cyber Security Requirements for DER provided as part of the onboarding process.

The common cyber security requirements aim to promote a level of cyber security capability across OEMs and Aggregators commensurate with the risks to the power system of cyber incidents involving DER. NSW and ACT DNSPs recognise that this is an area where both industry capabilities and national best practice are evolving. The DNSPs reserve the right to

- revise and update the common cyber security requirements from time to time to ensure NSW and ACT are aligned with national best practice and/or requirements imposed by State or Territory governments or the Commonwealth Government
- impose additional DNSP-specific requirements where an individual business deems this necessary.

In developing and updating the cyber requirements, the DNSPs' aim is to work collaboratively with industry in good faith to promote our common goal to ensure a safe and secure power system while also taking into consideration the needs and capabilities of industry.

5.4 Public Key Infrastructure (PKI)

NSW and ACT DNSPs' CSIP-AUS implementations require PKI aligned with the requirements of IEEE 2030.5:2018 Section 6.11. For further information on the process of generating and issuing certificates and the certificate structure, refer to the CSIP-AUS Explainer document.

The NSW and ACT DNSPs have adopted the common national PKI (NEPKI); OEMs and Aggregators will require NEPKI certificates to connect to production utility servers in NSW and ACT.

Prior to NEPKI, the NSW DNSPs have issued their own digital certificates via individual interim PKI solutions, to manage access to their utility servers for test and trial purposes. These interim PKI solutions are superseded by NEPKI and will be retired. Certificates issued through interim PKI will be supported in the production environment for a limited time only, as and if required to allow time for OEMs to migrate existing devices to NEPKI.

Notwithstanding whether certificates are issued directly by the DNSP or by NEPKI, the DNSPs reserve the right, without notice, to revoke certificates as part of a cybersecurity incident response.

5.5 IP whitelisting

Aggregator clients may require IP whitelisting to be able to connect to DNSP utility servers. Where IP whitelisting is required, both individual IP addresses and reasonable IP ranges are acceptable for whitelisting.

If an Aggregator is connecting via a whitelisted IP address and it intends to change its IP address, at least 20 days notice is required to the DNSP to make the necessary systems changes and maintain un-interrupted connectivity. Notice should be provided by email to the relevant DNSP's CSIP-AUS email address, as listed in section 5.1 above.

5.6 Ongoing obligations

The Utility Server Access Form in Appendix A sets out enduring expectations and obligations on parties connecting to DNSP Utility Servers, including in relation to cyber security. DNSPs reserve the right to revoke Utility Server access for any connecting party that does not abide by these obligations.

6 INSTALLATION AND COMMISSIONING

6.1 Overview

NSW and ACT DNSPs are aligning on a common installation and commissioning process based on best practice established through CSIP-AUS rollouts in other jurisdictions.

The following sections summarise key elements of the installation and commissioning process for CSIP-AUS products in NSW and ACT.

6.2 Site registration

Site registration is the process through which a new CSIP-AUS Software Communications Client representing a site is made known to the relevant DNSP's Utility Server. This process is the first step to be completed once the physical equipment installation is complete, and is a pre-requisite to performing the on-site capability test, described below.

For Direct Device clients this is only required once, for the EndDevice to register itself (and the ConnectionPoint that the EndDevice is associated with). For Aggregator clients, this will be required for each EndDevice that that the Aggregator Client is managing.

6.2.1 In-band registration

The first step in the registration process is typically initiated via the product vendor's mobile app or online portal. The installer will need to select the correct DNSP for the installation from within the app/portal.

Devices will be authorised as they initiate communications with the Utility Server by posting to the EndDevice endpoint as described in section 6.1.4 of CSIP-AUS.

Once the client is registered, the site NMI must be associated with the client's Long Form Device Identifier (LFDI). NSW and ACT DNSP utility servers support in-band registration using the ConnectionPoint registration extension described in section 11 of CSIP-AUS. This enables a quick and simple registration process whereby the installer enters the NMI into the vendor's mobile app or online portal and this triggers the client to message the Utility Server to create the association.

If the NMI received by the Utility Server is not a valid NMI for the DNSP in question, or if there is no record of an approved connection application for that NMI, the process will fail and feedback will be provided for the installer to check details and try again.

6.2.2 Out-of-band registration

In normal operations, installers will register new EndDevices through the in-band registration workflow described above. NSW and ACT DNSPs do not intend that installers should ever have to manually obtain and provide a device LFDI as part of the installation process.

The only cases where device registration data will be updated via an out-of-band process are:

- For Aggregators, once the onboarding process is complete and prior to connecting to the utility server for the first time, the Utility Server will create an EndDevice to represent the Aggregator and configure that EndDevice with suitable permissions. This process is described in section 4.1.4 of the CSIP-AUS Explainer document.
- If there is a need to remove or delete an EndDevice from the Utility Server it will be necessary to contact the DNSP to do this.
- In exceptional circumstances where the in-band registration process cannot succeed for a device, DNSPs will be able to create the necessary association within their servers manually to resolve the issue.

6.3 The installer portal

Unique to NSW is the common Installer Portal developed by the NSW Government which provides a single point of entry for installers to complete the on-site commissioning process regardless of which DNSP's service territory the installation is in. Having a common installer portal will help ensure a streamlined and consistent process for installers.

Endeavour Energy, Ausgrid and Essential Energy have worked with the NSW Government and the solar industry to co-design the NSW Installer Portal and have adapted their individual CER application and installation processes to align on a common process for NSW.

The NSW Installer Portal, as a NSW Government initiative, is not available for installations in the ACT. Evoenergy, the NSW Government and the NSW DNSPs have, however, worked

together to ensure that the installation process provided by Evoenergy in the ACT will mirror, as far as possible, the workflow and functionality of the NSW Installer Portal, so that installers operating across both NSW and the ACT have a consistent experience.

6.4 Capability test

Once the CSIP-AUS client has successfully registered with the DNSP Utility Server, the installer must perform an on-site capability test to validate that the site is able to communicate correctly with the server and to confirm that the export limiting functionality required for the NSW emergency backstop mechanism and for DNSP flexible exports schemes is working.

The NSW and ACT DNSPs have aligned on a common capability test procedure that is based on the procedure used in South Australia, the state that has the most experience with the CSIP-AUS site commissioning process.

Once the site registration process has completed, the installer will be able to activate the capability test using the Installer Portal. The test should typically take no more than five minutes to complete, during which time the installer will receive feedback on the progress of the test sequence through the portal. If the test fails for any reason, the portal will provide guidance as to the possible cause.

The capability test sequence for a typical small customer site is as follows:

- After site registration has occurred, the site will be temporarily configured with a 1-minute post/poll rate (DERProgramList pollRate = 60s, MirrorUsagePoint postRate = 60s). Setting these rates to 1 minute vs. the standard 5 minutes allows for the test sequence to complete as quickly as possible.
- The site will be set to a default export limit of 1.5kW (DefaultDERControl OpModExpLimW = 1500W) and a 100% ramp rate (setGradW = 100).
- The following test sequence will then be performed:
    - **Test 1: confirm connectivity**: this test confirms that telemetry has been received from the site. If no telemetry is received within 5 minutes, the test will fail.
    - **Test 2: confirm adherence to default limit**: this test monitors site active power telemetry (MirrorUsagePoint) to confirm that (a) there is some export from the site and (b) the level of export is within the default limit of 1.5kW. If there is insufficient export (< 500W) or if the export exceeds the default limit (+200W margin for fluctuations in site load) the test will fail.
    - **Test 3: confirm adherence to zero export limit**: the server will set a zero export limit (active control OpModExpLimW = 0) and then monitor site active power telemetry to confirm that a reduction in site export to zero (+/- 200W) is observed. If the required response is not observed within 5 minutes the test will fail.
- Once the test has passed, the active zero export control is cancelled and the post/poll rates are restored to the default 5 minutes. If the test fails, post and poll rates will remain at 1 minute for a 2 hour window to allow for the test to be repeated.

Some sites (e.g. with significant daytime loads) may not export during the day. For these sites DNSPs will offer an alternative capability test that uses a generation limit (OpModGenLimW) to test that the device is responding correctly to instructions.

While the above description is accurate as at April 2026, it should be considered illustrative only, as the capability test process is likely to evolve over time based on industry feedback.

7 IMPLEMENTATION REQUIREMENTS

7.1 Overview

This section provides additional implementation guidance and requirements for aspects that are not covered or are identified as implementation specific in CSIP-AUS or IEEE 2030.5.

Readers are reminded to familiarise themselves with the CSIP-AUS Explainer document. NSW and ACT implementations will implement the standard according to the conventions in that document unless specifically detailed otherwise below.

7.2 Generating LFDIs

For direct connections, the LFDI is determined by the device certificate.

Aggregators generating LFDIs for managed devices shall use the technology provider's Private Enterprise Number (PEN) as the last 8 digits in decimal form with leading zeros. This ensures the technology provider can manage global uniqueness within their device pool without concern of clashing with other Aggregators. This is similar to the generation of the mRIDType object.

An example LFDI is as follows where [XXXXXXXX] is the PEN:

AA402E1AD2D673BAE72163FEFAA05BFC[XXXXXXXX]

If your organisation does not already have a PEN allocated, you may request one from IANA. The process is simple and free.

7.3 Multiple FSAs, multiple programs and overlapping controls

Clients must support multiple FSAs and multiple programs as per CSIP. Treatment of overlapping controls is as set out in section 7 of the CSIP-AUS Explainer document.

7.4 Control priority

Inverters shall implement the prioritisation behaviours in AS/NZS 4777.2:2020 table 2.6, with disturbance withstand limits and operation of the automatic disconnection device prioritised ahead of all remote control interactions.

Where CSIP-AUS remote controls relate to the same behaviours as local controls, remote controls shall be prioritised over local controls, e.g. remote limit controls shall be prioritised over locally-configured limits.

Where CSIP-AUS remote controls relate to different behaviours from local controls, the local control behaviour shall still be enacted e.g. where a remote limit control is in effect, the system shall still enact locally-configured responses to frequency conditions, voltage conditions and power rate limits.

7.5 Control responses

The communications software client shall support the following control responses from IEEE 2030.5 Table 27. All other responses are excluded.

Enumeration Value	Description
1	Event received
2	Event started
3	Event completed
6	The event has been cancelled
7	The event has been superseded

7.6 Subscriptions

Where Aggregators are utilising subscriptions, they shall renew subscriptions every 24 hours.

7.7 Telemetry

The following average readings are required through the Metering Mirror function set:

- Site Real Power
- Site Reactive Power
- DER Real Power
- DER Reactive Power
- Site Voltage (DER voltage can be provided if site voltage is unavailable)

Average readings shall be generated in accordance with section 4.2.4 in the CSIP-AUS Explainer document.

7.8 Device status

Required DERStatus objects are listed below. For further information refer to section 4.3.2 in the CSIP-AUS Explainer document.

DERStatus objects	Requirement
OperationalModeStatus	Required for all implementations
GenConnectStatus	Required for all implementations
inverterStatus	Not required
alarmStatus	Not required

7.9 DER capability

Clients use the DERCapability resource to post nameplate ratings to the utility server as per the table below.

DERSettings	DERCapabilities	Aggregation
setMaxVA	*rtgMaxVA*	Total
setMaxVAr	*rtgMaxVAr*	Total
setMaxVArNeg	*rtgMaxVArNeg*	Total
setMaxW	*rtgMaxW*	Total

When multiple DER are being represented by one LFDI the values posted should represent the aggregate nameplate capacity of all managed devices at the site.

Clients are required to post:

- What modes are supported for the modesSupported bitmap such as opModEnergize
    - What CSIP-AUS controls have been implemented via the csipaus:doeModesSupported as per Section 9 of CSIP-AUS.

7.10 Post and poll rates

For normal operation the Utility Server will configure poll and post rates for resources as per the table below. Upon initial registration and if not otherwise specified by the Utility Server, these should be used by default:

Resource	Type	Value (secs)
Device Capability	Poll	900
EndDeviceList	Poll	900
FunctionSetAssignmentList	Poll	900
DERProgramList	Poll	300
DERList • ***DERStatus*** • ***DERSettings*** • ***DERCapability***	Post	300
MirrorUsagePoint	Post	300
EndDevice	Post	300

A CSIP-AUS utility server may remotely update client poll and post-rates for various resources. This functionality may be used by the DNSPs to:

- reduce DERControl poll intervals and measurement post intervals from the default of 5 minutes to minimise the on-site execution time for the capability test as described in section 6.4
- increase measurement post intervals to minimise data traffic in periods of reduced system security or distribution network risk
- reduce post intervals and/or poll rates for specific sites with high network impact or to support investigation of site-specific problems or network issues.

Aggregator implementations utilising the subscription/notification function set will have an ability to receive notifications of control events on change.

Telemetry posting should be at the specified post rate but ideally with a random offset from the 5-minute market interval (00:00, 00:05, 00:10, etc.) so that clients do not sent their updates to the sever at exactly the same time. Refer section 8.1 in the CSIP-AUS Explainer document.

7.11 Failure modes

It is imperative for the integrity of the power system that CSIP-AUS products behave correctly during the following kinds of events:

- Utility Server outages
- widespread communication outages
- power outages.

NSW and ACT implementations must conform with the requirements in sections 5.2 and 5.3 of the CSIP-AUS explainer document in these scenarios.

APPENDIX A

Utility Server Access Form

Part A – Company details

An online version of this form is available at https://forms.office.com/r/pumS8v1KKy. The online form is hosted by Ausgrid and it will share the completed details with all NSW/ACT DNSPs and NEPKI.

Entity name	
Australian Business Number (ABN)	
IANA Private Enterprise Number (PEN)	
IP address required for test server*	
IP address required for production server*	
Address	
Technical contact name	
Technical contact email	
Technical contact phone	
Equipment type (tick all that apply)	☐ Gateway ☐ Inverter
Software client type (tick all that apply)	☐ Cloud ☐ Direct
Name of authorised officer	
Title of authorised officer	
Email of authorised officer	

*Note: for cloud/Aggregator clients, the IP address (or address range) of the incoming connection to the utility server may be required for IP whitelisting. This can be provided later if not known at time of application.

Part B – Declaration

As the authorised officer named in Part A above, I confirm that the Company has read, understood, and will abide by:

1. The NSW-ACT Utility interconnection handbook (this document)	☐
2. The Common Cyber Security Requirements for DER (including completion of the declaration of conformance in Appendix A)	☐
3. The Utility Server Access Principles (Appendix B of this document)	☐

APPENDIX B

Utility Server Access Principles

The following Utility Server Access Principles were co-developed and agreed between NSW and ACT DNSPs and OEMs and Aggregators through the OEM Working Group convened jointly by ENA and ANU from mid-2025 to mid-2026. OEMs and Aggregators with devices connecting to NSW and ACT Utility Servers are expected to abide by these principles.

1. The OEM/Aggregator must maintain compliance with the utility interconnection handbook and the common cyber requirements
2. The OEM/Aggregator must notify the DNSP of any planned or unplanned outages or changes to its systems, software or firmware that may cause, or have caused, the OEM/Aggregator's clients to become disconnected from the utility server
3. The DNSP must notify the OEM/Aggregator of any planned or unplanned outages of its systems that may cause, or have caused, the OEM/Aggregator's clients to become disconnected from the utility server
4. The DNSPs and OEMs/Aggregators acknowledge:
    a. that their systems must have sufficient performance to maintain required poll / post rates for all connected clients during
        i. Normal operation
        ii. Emergency backstop activation.
    b. that DNSPs have obligations to conduct regular tests of the backstop capability
    c. that all parties should work together in good faith to resolve any performance or other issues identified that could impact on the customer experience or the emergency backstop capability.

APPENDIX C

Change log

Version	Date	Notes
1.0	November 2025	Initial version
1.1	May 2026	Added section 5.6 (Ongoing obligations) Updates to Appendix A (declaration form) and added online form link Added Appendix B (Utility Server Access Principles) Added Appendix C (Change log) Minor updates