06 November 2026

Submission on "TSO–DSO coordination: Operational requirements"

Transpower System Operator
By email: fsr@ea.govt.nz

Subject: Re: Feedback on TSO–DSO coordination – Operational requirements

Counties Energy supports practical, two-way coordination that strengthens system security while enabling efficient use of distribution-connected flexibility. As the electricity distributor and Distribution System Operation (DSO), we retain responsibility for local network operation and distribution constraints. Transpower's responsibilities as transmission grid owner should be distinguished from its System Operator responsibilities for national grid-level system security and real-time market operation.

Our responses support a practical, right-sized hybrid approach: common information and coordination arrangements, local operational accountability, proportionate implementation and preservation of investment in open standards. A priority for this work is agreement between the System Operator, distributors and retailers on a common dispatch hierarchy for competing instructions to the same resource (see our response to Question 1).

1.0 Counties Energy's Response

Consultation question	Counties Energy response
1. What should be changed, added or removed from the five operational requirements?	We support all five requirements, subject to the following refinements. They should establish interoperable operational foundations, not predetermine a centralised control model or impose new obligations ahead of the appropriate regulatory and funding decisions. **Requirement 1 — accountabilities:** Explicitly distinguish Transpower's grid-owner and System Operator functions, Counties Energy's distribution-network and DSO responsibilities, and the contractual control rights of retailers, aggregators and customers. Define decision rights, conflict resolution, escalation and restoration arrangements for normal, constrained and emergency conditions. National service activation must be

Physical
14 Glasgow Road
Pukekohe 2120
New Zealand

Postal
Private Bag 4
Pukekohe 2340
New Zealand

Energy Reimagined
0800 100 202
countiesenergy.co.nz

	coordinated with local network limits; neither commercial signals nor an interface specification should confer new control rights. Existing Code powers and protection obligations must remain clear. **Requirement 1 — dispatch hierarchy and primacy:** The process for establishing primacy where transmission and distribution actions could conflict should be a priority deliverable, and it should extend to retailers and aggregators. One resource, such as a hot water cylinder, battery or EV charger, can be instructed by the System Operator, the distributor and a retailer or aggregator at the same time. We recommend agreeing a single, published dispatch hierarchy between Transpower, distributors and retailers. We propose the hierarchy recommended in the Future Networks Forum's upcoming draft Dynamic Capacity Management (DCM) framework, which was adapted from the hierarchy Counties Energy negotiated with participating retailers for hot water flexibility. In order of precedence: 1. **System security (Transpower as System Operator):** automatic under-frequency load shedding, fast and sustained instantaneous reserve, and System Operator emergency instructions. Expected to be rare. 2. **Distribution network security (distributor and DSO):** network emergencies, storm response, unplanned outages, requests from Transpower acted on through the distributor, and any situation where a network limit is at risk of being breached. Expected to be rare. 3. **Customer protection:** limits on the cumulative restriction a customer experiences across all parties using their resources. Likely to apply. 4. **Local network management:** envelope-based management of local constraints and localised peak management, short of an emergency. Likely to apply. 5. **Third-party flexibility services (retailers, aggregators and flexibility service providers):** available most of the time. 6. **Distributor commercial participation:** only where the resource is not otherwise in use, and only without affecting any higher priority.

INTERNAL

	Why this ordering: The first two tiers record obligations that already exist, namely the System Operator's Code requirements and a distributor's obligation to operate its network safely, so the hierarchy confers no new control rights. Customer protection ranks above routine local network management so that the cumulative effect of every party's use is constrained, including the distributor's own. It does not override a genuine network limit, which escalates to distribution network security. Because the higher tiers are expected to apply in a minority of intervals, retailer and aggregator use remains available most of the time. A party whose instruction is deprioritised should be notified, with a reason, and application of the hierarchy should be auditable. The hierarchy should be applied consistently across distributors and enforced at the point of dispatch, so that retailers and aggregators face one rule set rather than one per distributor. **Requirements 2 and 3 — information:** Distinguish installed, approved, commissioned, connected, available, contracted and activated capability. Nameplate capacity is not dependable flexibility. Include response duration, energy limitations, confidence, rebound and competing commitments where relevant. Make reciprocal System Operator and grid-owner information an explicit deliverable, rather than a secondary consideration. **Requirement 4 — interoperability:** Separate common information semantics, transport interfaces and resource-control protocols. Counties Energy has built CSIP-AUS / IEEE 2030.5 capability through its Gridex DSO Orchestration Platform. An existing preference for OpenADR in related programmes should not become a default requirement for all TSO–DSO exchanges or force replacement of interoperable distributor investment. Ideal approach would be to assess standards against defined functions, whole-of-life costs and international adoption. Any chosen standard or protocol must also be assessed for security: an interface specification alone does not make a connection secure, and OT-grade protocols such as DNP3 or ICCP should not be exposed to unregulated consumer energy resource (CER)

INTERNAL

	connections. Any chosen interoperability protocol should also be tested and aligned with the Australian market (AEMO) to ensure a degree of consistency given the close proximity and OEMs selling in one market will want similar standards to apply in the other. **Requirement 5 — performance:** Retain outcome-based, risk-proportionate assurance. Communications conformance alone does not establish ride-through performance, physical delivery or firm availability. Define commissioning evidence, monitoring, exceptions and accountability for remediation. **Cyber security of the connection path:** Interoperability requirements must not be read as a requirement to bring all CER and distributed energy resource (DER) data into operational technology (OT) environments through SCADA, ICCP, DNP3, ADMS or similar protocols. CER technology providers and the security of their connections are not currently regulated, so a poorly secured device, original equipment manufacturer (OEM) cloud or gateway could become a route into distribution networks and, through them, the national grid. The obligation to secure each connection between devices, OEM clouds, gateways and utility systems must be defined and assigned before these IT-originating environments are connected to operational systems, so that distributor and Transpower networks and business processes are not compromised. See our responses to Questions 5 and 6. **Certificate management and a national PKI:** Secure, interoperable communication between utilities, aggregators, OEM clouds, gateways and devices depends on trusted digital identity. New Zealand needs a nationally governed public key infrastructure (PKI) management service for CER and DER, and for the system-to-system exchanges between Transpower and distributors. It should provide a common root of trust, organisation and device onboarding and validation, certificate issuance, renewal, revocation and status checking, and an audit trail. The alternative is fragmented, utility-specific or vendor-specific certificate arrangements, which would raise costs for OEMs and distributors, create inconsistent security outcomes

INTERNAL

	and be difficult to assure. We recommend the Electricity Authority, Transpower, distributors and the National Cyber Security Centre evaluate two options promptly: adopting or partnering with Australia's National Energy PKI (NEPKI), or establishing a locally developed national PKI for the New Zealand market. Either option should be not-for-profit, neutral and open to all participants on equal terms. It should be interoperable with Australian arrangements so that OEMs selling into both markets are not required to meet two separate regimes. NEPKI's current Australian authorisation is limited to CSIP-AUS communications, so its application in New Zealand and to other protocols would need to be confirmed. The PKI should not be tied to one protocol, vendor or platform. See our responses to Questions 5, 6 and 7. **Cross-cutting additions:** Establish transparent cost allocation, data-use permissions, consumer safeguards, neutral access and staged implementation. A network operating limit is not a purchased flexibility service: safety-related limits must not substitute for appropriately procured services where customers are being asked to provide an additional commercial response. Cyber security responsibility for each connection path, and a national PKI to manage certificates and device identity, should be defined as part of these foundations, not deferred.
2. For each information item listed, is the proposed source best placed to create and maintain an authoritative value?	The proposed sources are broadly reasonable, but listing several parties does not identify which party is authoritative for each field. Agree field-level ownership, provenance, validation and correction processes. The party holding data is not necessarily the party qualified to attest to its accuracy. **Embedded generation:** The distributor should be authoritative for connection approval, agreed connection limits and network location. Asset owners, installers and OEMs should supply installed equipment and verified commissioning characteristics. Electricity Authority-held information should be reused where fit for purpose, rather than recollected. **Battery capability:** Asset owners/OEMs should maintain ratings and technical characteristics; the distributor should maintain approved import/export limits. The controller or aggregator

INTERNAL

	should provide current state, availability and operational commitments. These are distinct values. **Large loads and data centres:** The customer/asset owner should provide expected operating profiles and changes; the relevant distributor or Transpower as grid owner should maintain connection capacity and the network interface. **Controllable demand and flexibility:** The party with contractual operational control should attest to available quantity, response and duration. Counties Energy can attest to its controlled-load arrangements and local network feasibility but should not be assumed to know all retailer or aggregator commitments behind the meter. **Network equivalents, topology and enduring constraints:** Each network owner should maintain its own network information. The System Operator should govern the integrated study assumptions and agreed boundary representation, with traceability back to source data. **Protection and technical performance:** Owners/OEMs should provide settings and test evidence; distributors and Transpower should validate the matters within their respective responsibilities. Material uncertainties should remain visible rather than being represented as verified compliance. **Dynamic MW/MVAr and forecasts:** Use the agreed boundary measurement owner for actuals, and identify the producer, assumptions and confidence of each forecast. Aggregator portfolio forecasts and distributor net grid exit point (GXP) forecasts should be reconciled, not treated as interchangeable. **Available/activated flexibility and DER state:** The controller/aggregator supplies availability, activation and device state; the distributor supplies applicable local constraints. Confirmation of message receipt must be distinguished from measured delivery. **Distribution events:** Counties Energy is authoritative for its faults, outages, constraints and loss of control capability. Transpower should reciprocally provide grid-owner outage/interface information and System Operator schedules,

INTERNAL

	warnings, relevant actions and restoration information through clearly assigned channels.
3. Is the proposed level of aggregation and timing proportionate to the operational use?	Broadly yes. GXP-level information should be the default for whole-system coordination where sufficient, with portfolio or material-asset detail only where a defined decision requires it. A GXP aggregate must not imply that all underlying flexibility is deliverable at every location or under customer agreements. Counties Energy still needs feeder, transformer and connection-point visibility to assess local constraints; the System Operator should normally receive the resulting feasible aggregate rather than duplicate that local operating function. Separate net demand, gross embedded generation where needed, and incremental flexibility to avoid double counting. State the measurement boundary, import/export sign convention, topology version and forecast assumptions. Standing information should update on approval, commissioning, material configuration change and decommissioning, supported by periodic reconciliation. Forecasts should use agreed day-ahead / intraday horizons. Event messages should be triggered by agreed materiality thresholds; operational telemetry should have use-case-specific latency, availability and quality requirements. A five-minute exchange could be tested for scheduling use cases but should not be treated as sufficient for fast protection or frequency response. For constrained or emergency operation, include effective start/end times, acknowledgement deadlines, expiry, stale-data flags and fallback behaviour. Share state of charge at portfolio level unless individual-asset detail is necessary. Allow proportionate pathways for smaller distributors without weakening assurance for services relied on for security.
4. Which requirements can already be met through existing information, systems or processes?	Existing connection applications, ICP/registry information, network models, outage processes, operational contacts, System Operator publications and established emergency arrangements provide a starting point for Requirements 1–3 and 5. Their coverage and quality should be assessed before imposing new collection or integration requirements.

INTERNAL

	Counties Energy's Gridex DSO Orchestration platform, in-flight Retailer Hot Water Flexibility Service, Karaka Harbourside Scaled Demand Flexibility Pilot and multiple other BESS can provide a practical foundation for Requirements 1- 4. Requirement 5 can be developed as required. These foundations should be reused, not interpreted as proof that every proposed national exchange, service level or certification requirement is already met. In particular, a standardised Transpower–Counties Energy interface, common forecast definitions, agreed operational primacy and end-to-end performance assurance still require joint definition and testing. Existing SCADA, ICCP and ADMS connections are secured within the OT environment on the basis of known, accountable counterparties. That assurance should not be extended by default to CER and DER data sources. Reusing these systems for CER and DER data should be conditional on a defined security architecture, not assumed to be fit for purpose. Start with a shared capability inventory mapping each proposed data field and use case to an existing source, interface, responsible party and known limitation. Avoid parallel DER registers and repeated bilateral reporting. Reuse existing demand-response integrations where fit for purpose, while allowing distributors with CSIP-AUS capability to connect through an agreed upstream interface rather than rebuild their resource-facing infrastructure.
5. Where are the material information, quality, access or capability gaps?	**Resource visibility:** Connection approval does not establish commissioning, current firmware/settings, continued connectivity or present control rights. Legacy and non-communicating resources require explicit estimates and uncertainty flags. **Location and identity:** Common mappings are needed between ICP, device, controller, portfolio, transformer/feeder and GXP, including topology changes and changes of retailer or aggregator. Incorrect mapping can make apparently available flexibility unusable for the relevant constraint. **Deliverability and firmness:** A shared view is needed of response duration, energy headroom, customer override,

INTERNAL

	communications status, rebound, baseline methodology, competing commitments and measured delivery. Flexibility relied on operationally needs contracts, assurance, dispatch rights and performance evidence; price responsiveness alone is not firm capacity. **Dispatch primacy:** There is no agreed, common order of precedence when the System Operator, a distributor and a retailer or aggregator can each instruct the same resource. Without one, each party must assume how conflicts are resolved, a deprioritised party may not know its instruction was overridden, and flexibility counted as available by one party may be consumed by another. The hierarchy proposed in our response to Question 1 should be agreed between Transpower, distributors, retailers and aggregators, and enforced consistently at the point of dispatch. Open points to resolve are: • how a distributor's operating envelope interacts with a System Operator instruction beyond under-frequency load shedding and reserves; • how customer manual override is treated; and • precedence between multiple aggregators at one site. **Two-way access:** Distributors need timely access to relevant grid constraints, voltage/interface conditions, planned outages, restoration status and material dispatch actions affecting their networks. Data access, permitted use, confidentiality, customer authorisation where required, and revocation must be operationalised. **Interoperability and resilience:** The gaps include common data objects, version governance, certificate/identity arrangements, acknowledgement and rejection codes, audit trails, fallback behaviour and end-to-end testing across standards. Translating a signal is insufficient if its units, primacy, validity or meaning changes. **Cyber security and the IT/OT boundary:** Providing all CER and DER data through SCADA, ICCP, DNP3 and similar protocols brings equipment and connections that are not regulated for cyber security into environments that protect distribution networks and the national grid. CER technology providers are not subject to regulated security requirements, and a

INTERNAL

	compromised device, cloud or gateway could introduce a backdoor into distributor and Transpower systems. There are three connection architectures, and the exposure differs for each: • **Device to server:** The utility server communicates directly with the device. The utility controls its own end of the connection, but device-level security (authentication, certificates, firmware integrity and update practices) still rests with the device manufacturer. • **Device via an intermediary OEM cloud to server:** The OEM becomes responsible for securing the device-to-cloud link, the cloud platform and its access controls. The utility can only see and trust the OEM-to-server leg. There is no standard, validation or testing of the OEM leg. • **Device to gateway to server:** The gateway is responsible for securing the device-to-gateway link and for the integrity of the gateway itself, including its firmware, credentials and remote access. There is no standard, validation or testing of gateways either. In the second and third architectures, security depends on OEM obligations that are currently undefined, unassured and unenforceable by distributors. The obligation to secure connections between devices and their cloud or gateway must be defined, assigned and testable before these IT environments are connected to OT environments. Without this, a security failure at one OEM could affect many networks at once. We recommend that the Electricity Authority, Transpower, the Commerce Commission and distributors, in consultation with the National Cyber Security Centre, agree: • minimum security requirements and responsibilities for each of the three architectures, including OEM obligations for cloud and gateway security; • **a national PKI management infrastructure** to assure certificate management and security across all three architectures, covering organisation and device onboarding, certificate issuance, renewal, revocation and status checking, and a shared root of trust. This could be

INTERNAL

	Australia's National Energy PKI (NEPKI) or a national PKI developed locally for the New Zealand market, but it should be nationally governed and consistent, rather than a set of separate distributor or vendor arrangements; • independent validation, certification and testing of devices, gateways and OEM platforms before they are permitted to connect; • a defined security boundary, such as a demilitarised zone or an application-layer interface, so that CER and DER data is received into IT or DER management systems and only validated, aggregated information reaches SCADA, ICCP or ADMS; • accountability, incident notification and isolation arrangements, so that a distributor or Transpower can disconnect a compromised path without losing network visibility or control. **Implementation economics:** Clarify who pays for additional telemetry, integration, ongoing assurance and 24/7 support, and how efficient expenditure can be recovered. A requirement should become mandatory only after its operational benefit, cost, responsibility and transition pathway are established. Capability gaps should be addressed through staged delivery, including shared services where appropriate, rather than assuming every distributor is at the same maturity.
6. Which initial information exchange(s) should be prioritised for early definition or trial?	Prioritise a bounded, two-way Transpower–DSO trial with agreed accountabilities before choosing an enduring national platform. Counties Energy's existing DSO Orchestration platform with CSIP-AUS capability offers a useful test environment, subject to agreed scope and resourcing. **First — reciprocal constraints and event notifications (or DOEs):** Exchange relevant GXP/grid-interface constraints, outages, significant distribution events, warnings, restoration status and loss of control capability. Establish common identifiers, effective times, acknowledgement, escalation and fallback procedures. **Second — feasible flexibility availability and activation:** Counties Energy or the controlling participant supplies feasible aggregate MW, direction, duration, response time, confidence

INTERNAL

	and recovery profile at the agreed GXP/portfolio boundary. A request is checked against current distribution limits; acceptance, partial acceptance or rejection includes a reason, expiry and audit trail. Verify physical delivery separately from acknowledgement. Test overlapping retailer, aggregator, distributor and System Operator requests without assuming a new role allocation or displacing existing Code arrangements. Use the dispatch hierarchy proposed in our response to Question 1 as the baseline for these tests and verify that a deprioritised party is notified with a reason. **Third — net-GXP forecasting:** Reconcile actuals and forecasts with embedded generation, battery behaviour and expected demand response. Explicitly account for activated flexibility and its rebound so that dispatch is not counted twice. For the upstream interface, assess a limited aligned profile for resource groups, availability, forecasts and dispatch-related exchanges; retain CSIP-AUS downstream. **Cyber security conditions for the trial:** The trial should use a controlled security architecture and test all three connection paths (device to server, device via an OEM cloud to server, and device to gateway to server) before any CER or DER data reaches operational systems. Trial data should enter through an IT-side or demilitarised boundary. The trial should document who is responsible for security on each leg and test authentication, certificate management, logging, and the isolation and recovery of a compromised path. It should also test certificate onboarding, issuance, renewal and revocation using a PKI service that is a candidate for national use, whether NEPKI or a locally developed New Zealand PKI. This would show whether a national PKI management infrastructure is workable in New Zealand before any enduring arrangement is chosen. Its findings should be published so that minimum requirements for OEMs and gateway providers can be defined. Measure avoided integration effort, data completeness, forecast improvement, response latency, delivery accuracy, rejection handling, consumer impacts and communications-loss performance. Test potentially disruptive scenarios in simulation

INTERNAL

	or a controlled environment, with operational approval and stop criteria. Publish reusable specifications and lessons before scaling.
7. Are there relevant initiatives or standards we should align with to avoid duplication?	**New Zealand policy alignment:** Coordinate this work with the Electricity Authority's DSO roadmap, MOSP/Data Hub Manager work, DER visibility, smart-inverter and flexible-export workstreams. Our previous submissions favour a practical hybrid approach, contract-backed flexibility, retailer alignment and a federated data-exchange capability rather than unnecessary central duplication. A data hub can enable discovery, authorisation, addressing and auditability; it should not automatically become a central DER controller. **CSIP-AUS IEEE 2030.5:** Recognise Counties Energy's built capability and the Australian implementation ecosystem. CSIP-AUS provides a common profile for utility–DER communications, including operating-limit applications. Specify versions, supported functions, New Zealand ICP mapping and end-to-end tests rather than relying on a generic compliance label. This supports reuse of the equipment and aggregator ecosystem already developed for the Australian market. **Dynamic Capacity Management (Future Networks Forum):** Align the TSO–DSO dispatch hierarchy with the upcoming draft DCM framework being developed through the Electricity Networks Aotearoa Future Networks Forum, which recommends a common control hierarchy across distributors. The draft is consistent with Australian practice, where SA Power Networks' Market Active Solar trial prioritises the distributor's operating envelope over retail signals. Counties Energy supports a single hierarchy covering both TSO–DSO coordination and distributor–retailer dispatch, so that the two efforts do not diverge. **Cyber security standards and assurance:** Alignment should also cover cyber security frameworks, device and gateway security certification, and OEM cloud security requirements. CSIP-AUS IEEE 2030.5 define how information is exchanged, but none of them resolves who is accountable for the security of an OEM cloud or gateway, or validates it. New Zealand should learn from

INTERNAL

	Australian and international work on CER cyber security and agree minimum requirements, testing and accountability for OEMs and gateway providers before CER and DER connections are integrated with SCADA or ADMS environments. **National PKI (Australia's NEPKI):** Australia has established the not-for-profit National Energy PKI (NEPKI) to procure and operate a single national PKI service for CSIP-AUS clients and servers. It replaces utility-specific certificate arrangements and gives OEMs one onboarding path, with certificates issued under a common root of trust and managed through their lifecycle. New Zealand should assess NEPKI against a locally developed national PKI for the New Zealand market, considering governance, cost to OEMs and distributors, local oversight, and the ability to support protocols other than CSIP-AUS and exchanges between Transpower and distributors. Whichever is chosen, it should be national, neutral and interoperable with Australian arrangements, so that OEMs selling in both markets can meet one consistent certificate and security regime. Counties Energy's CSIP-AUS / IEEE 2030.5 capability would benefit directly, because secure, standards-based communications depend on trusted certificate management. Our recommendation is a layered, standards-based architecture: governed TSO–DSO information exchanges; distributor assessment and orchestration within local network limits; and interoperable aggregator/device communications. Adopt common outcomes and profiles without mandating one vendor, one platform or unnecessary changes to existing open-standard investment.
8. Do you agree with the priority use cases that we have identified? If not, which would you consider are higher priority?	Yes. All five use cases are relevant and well prioritised.

Ngā mihi,

Counties Energy

INTERNAL