Tasmanian Networks Pty Ltd
ABN 24 167 357 299
PO Box 606
Moonah TAS 7009

6 September 2019

Mr John Pierce
Chair
Australian Energy Market Commission
PO BOX A2449
Sydney South NSW 1235

Via online submission

Dear Mr Pierce,

RE EPR0057 – DISCUSSION PAPER ON MECHANISMS TO ENHANCE RESILIENCE IN THE POWER SYSTEM

TasNetworks welcomes the opportunity to make a submission to the Australian Energy Market Commission's (**AEMC**) discussion paper on mechanisms to enhance resilience in the power system.

As the Transmission Network Service Provider (**TNSP**), Distribution Network Service Provider (**DNSP**) and jurisdictional planner in Tasmania, as well as the proponent considering the feasibility of the Marinus link, TasNetworks is focused on delivering safe and reliable electricity network services while achieving the lowest sustainable prices for Tasmanian customers. All of these roles require the prudent, safe and efficient management and development of the Tasmanian power system. TasNetworks is therefore supportive of AEMC's efforts to investigate mechanisms to enhance resilience in the national power system.

TasNetworks supports Energy Networks Australia's (**ENA**) submission and would like to make several further comments with a particular focus on the Tasmanian context. The key points in this submission are:

- TasNetworks agrees that the system security framework should be reviewed to ensure Network Service Providers (**NSPs**) and the Australian Energy Market Operator (**AEMO**) have the appropriate tools to manage power system risks. This includes those resilience risks which are evolving as a result of the energy transition, from indistinct events as defined in the Discussion Paper as well as the additional considerations offered in this submission.
- TasNetworks considers that the principles comprising the Commission's assessment framework are appropriate. However, TasNetworks suggests that there may be benefits in considering a broader view of resilience to capture High Impact Low Probability (**HILP**) concerns as well as other identifiable risks from credible and non-credible contingencies.
- Crucial to this view is recognition of the inherent complexity and uncertainty associated with management of the power system as the grid transitions towards an increasing penetration of intermittent, weather dependant, inverter connected generation types.
- This needs to be supplemented with a recognition that it is not economic, nor practical, to protect against all risks, all of the time. In this respect, TasNetworks contends that efforts to

improve resilience should be commensurate with practical and economic realities, and an agreed 'risk appetite'.

- If changes to rule definitions are envisioned to enhance resilience, TasNetworks cautions that these must be carefully considered so that unintended consequences are avoided. It may prove safer and easier to separate discrete and non-traditional indistinct events, and deal with the latter within its own framework.
- TasNetworks suggests the issue of uncertainty created by the response characteristics of Distributed Energy Resources (**DER**) to network fault events needs further clarification and consideration given its potential to materially exacerbate the severity of both credible and non-credible contingency events.
- TasNetworks considers the application of pre-determined, variable safety margins within existing constraint equations might be one potential mechanism for improving system resilience. These would reflect the level of 'confidence' in the power system at any given time such that increased safety margins could be invoked.
- As operation of the power system becomes more complex, there must be appropriate valuation and recognition of technical skills and resourcing at all levels to ensure that issues like resilience, and concepts like the General Power System Risk Review, can be adequately resourced and implemented.
- TasNetworks considers that indistinct events should be evaluated as part of the planning process for non-credible contingency events. To this end, TasNetworks supports a review of the protected events framework so that a more robust and consistent risk management approach results.
- Notwithstanding this support, TasNetworks acknowledges that accurately defining indistinct events and quantifying their probability will be challenging. As such, TasNetworks suggests consideration be given to the value of introducing a set of published 'system design criteria' for each region. Such criteria would clearly articulate the contingencies that 'must' be adequately managed, and by omission, would then define what remaining contingencies are to be managed on the basis of 'best endeavours'.
- TasNetworks is not adverse to the monitoring and publishing of interconnector flows including provided it is not commercially sensitive. However, TasNetworks does not consider the introduction of a formal interconnector flow standard is required given the need to manage power flows within the existing system security framework.

TasNetworks responses to individual questions are provided below and we welcome the opportunity to discuss this submission further with you. Should you have any questions, please contact Andrew Halley, Principal Operations Engineer, via email (andrew.halley@tasnetworks.com.au) or by phone on (03) 6271 6759.

Yours sincerely,

Chantal Hopwood

Leader Regulation

QUESTION 1: ASSESSMENT FRAMEWORKS
Do stakeholders agree with the Commission's assessment framework?

TasNetworks considers that resilience is an important risk management concept that is not well captured by the existing rules. This is largely due to the historical focus on discrete events which can be clearly defined both ahead of, as well as during, real time operation of the network. TasNetworks therefore supports the Commission's investigation of this issue and agrees that the principles comprising the Commission's assessment framework are appropriate. However, TasNetworks suggests these principles would be usefully informed by consideration of the following broader points on resilience and uncertainty.

Notwithstanding footnote 25 on page 21, the discussion paper is weighted towards management of High Impact Low Probability (**HILP**) events. TasNetworks notes that this is not inconsistent with the statement of resilience found in the Commonwealth Government's Critical Infrastructure Resilience Strategy[1]. However, TasNetworks suggests that there may be benefits in considering a broader view of resilience to capture both HILP concerns as well as other identifiable risks from credible and non-credible contingencies. For example, from sympathetic tripping of Distributed Energy Resources (**DER**) discussed further below. For consistency with Chapter 3 of the Discussion Paper, resilience might be better characterised as allowing the power system to cope with, and respond appropriately to, events which are more onerous than anticipated due to increasing levels of uncertainty occurring in operational timeframes.

Crucial to this view is recognition of the inherent complexity and uncertainty associated with management of the power system as the grid transitions towards an increasing penetration of intermittent, weather dependant, inverter connected generation types. This includes significant levels of DER and, in particular, rooftop photovoltaics (**PV**).

TasNetworks considers that acceptance by all National Energy Market (**NEM**) stakeholders, including Governments and market bodies, that inherent errors, ongoing uncertainty and residual risk will be unavoidable when weighing realistic solutions to these challenges. In particular, for decisions made through necessity in operational timeframes. This needs to be supplemented with a recognition that it is not economic, nor practical, to protect against all risks, all of the time. As alluded to in Section 3.3.1 of the Discussion Paper, what constitutes an appropriate 'risk appetite' is therefore another important matter for consideration. In this respect, TasNetworks contends potential solutions should be commensurate with practical and economic realities and exhibit an appropriate degree of flexibility. That is, exactness should not be sought where only an approximation of the underlying issues is possible at the outset.

QUESTION 2: CONTEXT AND BACKGROUND
Do stakeholders agree with the staff view on the need to extend system security frameworks to clearly manage risks from indistinct events?

TasNetworks agrees that the system security framework should be reviewed to ensure NSPs and AEMO have the appropriate tools to manage power system risks. This includes those resilience risks which are evolving as a result of the energy transition, from indistinct events as defined in the Discussion Paper as well as the additional considerations offered in this submission.

Whether the appropriate mechanisms are best facilitated through changes to the existing rules, or require the creation of new frameworks, is a matter for further consideration as part of the review process. Irrespective of the direction taken, TasNetworks considers that the outcome should be

[1] Of specific note is the statement under objective 3: "Of particular concern are low-frequency, high-impact events which, due to their rarity, may not be treated with a high priority until they occur. The Australian Government has a strong interest in promoting an understanding of, and preparation for, severe, national-scale crises, given its unique role in responding to such events."

transparent, robust and provide a consistent, risk based approach that can be applied to manage power system security when material uncertainties are identified.

If changes to existing rules are envisioned, TasNetworks cautions that these must be carefully considered. This is so that unintended consequences are avoided. By way of example, the impacts of any change to an existing definition such as '*credible contingency event*' would need to be precisely determined given its broad referencing throughout the rules, particularly in the technical schedules of Chapter 5.

Consideration also needs to be given as to how to best capture the uncertainty associated with indistinct events and, further, whether the associated issues are best solved in operational or planning time frames. For example, should indistinct events be included in the assessment of a Generator Performance Standard or should it be limited to the definition of what a *secure operating state* is in real time?

Given these considerations, there may be merit in separating discrete and non-traditional indistinct events, as depicted in Figure 4.3 of the Discussion Paper, and dealing with the latter as a separate, issue within its own framework. This might be an extension to the existing rules which would have clear lines of delineation to avoid significant impacts on other rule requirements. TasNetworks considers the first paragraph of Section 3.2 is an appropriate position from which deliberations should be commenced on this point.

In terms of relevance for the Tasmanian power system, there are a number of Renewable Energy Zones (**REZs**) likely to be developed that will host significant wind capacity in relatively compact geographical areas. The potential for highly correlated responses to prevailing weather conditions are expected. As such, it is important that the Tasmanian power system can be maintained in a *secure operating state* and not be allowed to 'drift' outside of its *technical envelope* under reasonably foreseeable circumstances. It is on this basis that TasNetworks considers there is merit in reviewing the mechanisms available to ensure that system security is not inadvertently compromised. This may be through dynamic operating margins, event reclassification or other actions available to AEMO.

Further to this point, TasNetworks suggests the issue of uncertainty created by the response characteristics of DER to network fault events needs further clarification. There is mounting evidence to suggest that an unknown percentage of DER will likely disconnect when subjected to a network disturbance[2]. This has the potential to materially exacerbate the severity of both credible and non-credible contingency events. Although 'wind farm feathering' has been discussed at length in the Discussion Paper, it is unclear whether the AEMC has a view on the risks from DER disconnections.

It is also unclear how such a network response is best treated under the existing security framework. For example, is it appropriate to use the reclassification of contingency events under 4.2.3A, noting that the risk is present day after day rather than being relevant for short, discrete periods of time such as during storms or bushfire events? Or does the new situation warrant classification as an *abnormal condition,* albeit that DER is always present and is now very much part of the 'normal' modern power system?

Given these questions, TasNetworks recommends that the issue of DER response uncertainty be elevated in significance as part of the ongoing resilience review. In order to explore how DER might impact system resilience and could be better evaluated, TasNetworks offers the following questions for consideration:

[2] As noted by the AEMC in Appendix F.3 of the Discussion Paper. TasNetworks also highlights another recent example from overseas where approximately 500 MW of DER was reported to disconnect as part of an under frequency load shedding event which occurred in the United Kingdom on 9 August 2019. For further information, please see: https://www.nationalgrideso.com/document/151081/download

- What MW contribution is coming from DER at any point in time? For example, PV without energy storage will be zero overnight. It can be noted that the answer to this question will progressively change as more PV is connected to the network. Further, newer technologies may have different risk profiles compared to the legacy systems already in service. Ongoing review and refinement to the aggregate risk profile is therefore likely to be required.
- How much of the DER is at risk of disconnection for a given contingency event? There will almost certainly be a locational aspect to this issue, with a likely overlap with particular discrete contingency events already defined as, and part of, existing power system security assessments.
- Does the risk of disconnection increase depending on surrounding network conditions, e.g. available system strength? Voltage disturbances are likely to propagate further and be more severe, in terms of magnitude of voltage depression, when the network is operating toward the lower end of its allowable system strength (fault level) range.

QUESTION 3: MANAGING VARIABILITY ARISING FROM CREDIBLE INDISTINCT RISKS
Do stakeholders agree that the criterion for a secure system requires amendment to account for risks arising from generation variability due to indistinct weather events? How do stakeholder see a probabilistic approach being applied in practice and integrated into AEMO operational practices, such as forecasting and pre-dispatch? What characteristics of variability should apply to the variability qualifying for management under system security arrangements (speed, and significance)? What governance arrangements and arrangements for transparency, such as the issuance of market notices, should apply to this process?

Consistent with the sentiments outlined above, TasNetworks considers that there is merit in reviewing the criterion used to define a *secure operating state*. However, the practicalities of applying complex solutions in a pre-dispatch and operational environment should be respected. That is, excess complexity should be avoided.

One potential mechanism for inclusion into operational practices might be the application of pre-determined, variable safety margins within existing constraint equations. These would reflect the level of 'confidence' in the power system at any given time. Highly variable periods of generation output, driven by prevailing weather conditions or assessed exposure of DER to potential disconnection, could be reflected in a lower confidence rating which would invoke an increased safety margin. For example, by:

- increasing Frequency Control Ancillary Services (**FCAS**) regulation requirements by 'X' MW during highly variable wind conditions,
- increasing contingency FCAS raise requirements by 'Y' MW during daylight hours when PV output is significant, and/or
- decreasing interconnector flow limits by 'Z' when power transfer levels are volatile due to the relative location of intermittent energy sources.

Such an approach would allow for greater 'drift' between the intended outcomes as determined by the National Electricity Market Dispatch Engine (**NEMDE**) and the actual state of the power system, over the course of a dispatch interval, without unmanaged risk. However, consistent with current market practices, TasNetworks considers that timely notification to market participants of any changes in the forecast 'headroom' underpinning the triggering of such mechanisms would be appropriate. For enduring indistinct events such as DER disconnection, it could be appropriate to use published 'standing advice' which is subject to periodic review to ensure its ongoing adequacy. If adopted, TasNetworks considers a key objective should be to minimise additional reporting burdens on AEMO for risk items which are continuous, albeit variable, in nature.

QUESTION 4: EXPANDING THE EXISTING POWER SYSTEM FREQUENCY RISK REVIEW
What are stakeholder views on incorporating all assessment of system service requirements (inertia and fault level) as part of the single risk review process? Incorporating DNSPs as formal members of the process in order to capture risks associated with high levels of DER? How an expanded GPSRR would be integrated with other AEMO planning processes, notably the ISP? How the GPSRR should best facilitate a time efficient process of identifying risks and implementing arrangements to manage those risks (through the declaration of a protected event, or RIT-T/D)? How frequently should the GPSRR be published - would a yearly publishing requirement adequately balance the time required for AEMO conduct a thorough review, against the need to regularly capture the changing risk profile of a transitioning power system?

Conceptually, TasNetworks appreciates the intent to expand the Power System Frequency Risk Report (**PSFRR**) into a General Power System Risk Review (**GPSRR**) so that a comprehensive assessment of all security risks in the national power system can be produced. TasNetworks agrees that DNSPs should be included as part of this process and can see advantages from a regular publication schedule. For example, this would allow timely responses to emerging issues to be developed and communicated as part of NSP Annual Planning Reports (**APR**) and AEMO Integrated System Plan (**ISP**) processes.

Practically however, TasNetworks has concerns about the time and effort required to undertake such an assessment on a 12-monthly cycle. In particular, on assessments related to non-credible contingencies which are inherently broader in scope and involve a greater number of variables than credible contingencies. Further, as the proposed scope of the GPSRR extends to issues including system strength, it would be necessary to use electromagnetic transients (**EMT**) simulation tools which are more complex to execute and much slower to run. This is in contrast with tools typically used for frequency stability studies, such as Power System Simulator for Engineering (**PSS/E**), which allow for more rapid calculations and analysis.

More broadly, it is important to note that the energy market transition is generating significant additional workload for NSPs on multiple fronts. Examples include increased regulatory activity stemming from changing rules frameworks and reviews, substantially increased volumes of generation connection enquires and applications, increased analysis to manage more complex system security risks arising from the integration of new power electronic based generation technologies and the increasing role of DER in power system dynamics. This is playing out against a significant focus on energy affordability. Moreover, TasNetworks considers this is being exacerbated by a resourcing and skills challenge which has not had sufficient focus and attention to date.

As operation of the power system becomes more complicated, there must be appropriate valuation and recognition of technical skills at all levels to ensure that issues like resilience, and concepts like the GPSRR, can be adequately resourced and supported.

QUESTION 5: ENHANCING THE EXISTING PROTECTED EVENTS FRAMEWORK
The governance arrangements for standing protected events and formal protected operation are equivalent to those currently in place for protected events: does this give AEMO sufficient ability manage foreseeable security risks? Does this provide appropriate oversight from the Panel? Should additional requirements be included? The proposed arrangements give AEMO an ad-hoc power to declare a period of protected operation for indistinct events during abnormal conditions: does it give AEMO sufficient ability manage unforeseeable security risks? What information should to be included in market notices? What post event reporting requirements should be placed on AEMO? Are there sufficient links to the GPSSRR? Is additional oversight required (e.g. the Panel)?

TasNetworks considers that indistinct events should be evaluated as part of the planning process for non-credible contingency events. To this end, TasNetworks supports a review of the protected events framework so that a more robust and consistent risk management approach results. To enhance transparency, this might be overseen by the Reliability Panel.

Notwithstanding this support, TasNetworks acknowledges that accurately defining indistinct events and quantifying their probability will be challenging. Given that it is impossible and uneconomic to guard against all HILP events, TasNetworks suggests consideration be given to the value of introducing a set of published 'system design criteria' for each region. Such criteria would clearly articulate the contingencies that 'must' be adequately managed, both with and without emergency control mechanisms including the use of System Protection Schemes (**SPS**)[3]. By omission, this would then define what remaining contingencies are to be managed on the basis of 'best endeavours'. In clearly identifying what the system has been designed to cope with, a better understanding and acceptance of risk, and risk outcomes, would be promoted across the entire stakeholder base.

QUESTION 6: INTERCONNECTOR STANDARD

What are stakeholder views on the value of and rationale for monitoring and reporting on interconnector flows? The proposed approach to monitoring and reporting on interconnector flows? The proposed role for the Reliability Panel in developing an interconnector flow standard?

TasNetworks is not adverse to the monitoring and publishing of interconnector flows including the extent to which operating limits are approached or breached. These would provide insight of encroachment into defined operating margins without necessarily resulting in an insecure system. However, this should only occur where publication of such information is not commercially sensitive and would not confer any commercial advantage/disadvantage to any market participant.

Notwithstanding these sentiments, TasNetworks does not see a requirement for a formal interconnector flow standard to be developed given the need to manage power flows within the existing system security framework. However, it is important to recognise that such comparisons may not always provide a definitive insight into *all* system security risks. For example, increasing 'drift' may have equally negative impacts on critical intra-regional constraints that may be as significant as interconnector flows. On this basis, TasNetworks suggests it may be worth considering whether analysis and reporting on other aspects of the power system should also be considered. That is, on real time operational outcomes versus constraint limits other than those associated with regional interconnectors.

As with the GPSRR comments above, if additional monitoring and reporting is to be pursued, resourcing impacts to facilitate development and ongoing application would need to be recognised and accounted for.

[3] For reference, CIGRE Technical Brochure 187 "System Protection Schemes in Power Networks" (Task Force 38.02.19, June 2001) adopted the use of System Protection Scheme in preference to Special Protection Scheme. The TB states that "*It was, however, clear to the task force members that 'special' has a relative meaning – what is special today will be common tomorrow, etc., and we found it more relevant to distinguish between equipment protection, such as line, busbar, transformer and generator protection, compared to system protection*".