8 August 2023

To the Department of Prime Minister and Cabinet
National Security Group Department of the Prime Minister and Cabinet
Level 8 Executive Wing
Parliament Buildings
Wellington 6011

Vector Submission – Strengthening the Resilience of Aotearoa New Zealand's Critical Infrastructure System

Vector's submission may be publicly disclosed.

Executive Summary

Whilst the specific proposals of the discussion document are not exactly clear, the changes contemplated by the Department of Prime Minister and Cabinet (DPMC) are potentially far reaching.

We support the goal of enhancing alignment across regulatory regimes relevant to critical infrastructure. This is one of the reasons why we oppose the establishment of a new regulatory regime for resilience overseen by a new critical infrastructure resilience agency.
Creating new requirements – and government entities – would reduce rather than improve coordination across regulations. For many critical infrastructure entities this would also duplicate requirements, and compliance costs, adding little additional value towards resilience. Perversely this would exacerbate an existing weakness of our current regulations – which is a lack of funding for resilience. In its default price pathway the Commerce Commission does not directly fund resilience expenditure – instead it determines allowable revenue by linking price and a narrow measure of *reliability.* In doing so it is orientated towards the goal of achieving marginal efficiency gains over time, by penalising overspending and imposing restrictions on financeability. This regime is inflexible in responding to many of the risks that this discussion document sets out and is the opposite of what is needed to meet the investment challenge in front of our sector in the context of climate change.

Given the role of existing regulations and requirements for some critical infrastructure entities, we consider that the true opportunity to improve resilience by way of regulation, is to align existing regulations to this goal – rather than to create a new regime. We understand the government's desire for assurance of consistent performance across critical infrastructure entities in an emergency. We therefore recommend that any new requirements are targeted on the basis of current critical infrastructure performance, and, the existence of any existing regulations. Undertaking such a gap analysis of infrastructure performance to inform any new requirements would help ensure additionality and avoid duplication (or cross-cutting regulations). We consider it would be valuable for the DPMC to recognise the existing work of many critical infrastructure entities to assess, manage, and publicly report against risk. This would help target any new requirements to where they are needed – and we believe would shed light on the impracticalities

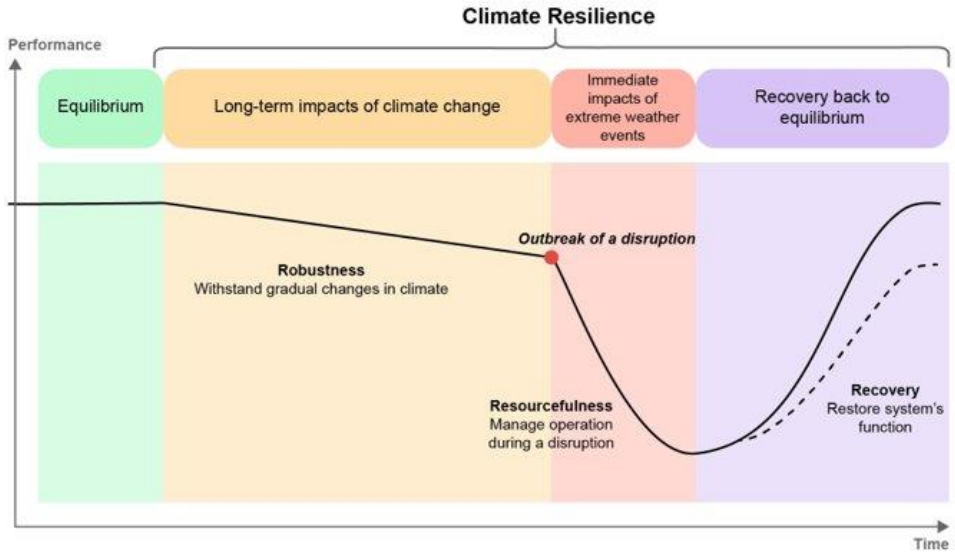
of imposing a new resilience standard across all critical infrastructure entities – given the diverse and technical operational realities across these entities. The challenge of introducing a new resilience standard is exacerbated by the fact that the risk environment of 2023 is shifting at a rate far more rapid than the possible pace of regulatory change. In this context there is a very real risk that in seeking to lead industry resilience efforts, a new regulatory regime in fact slows such efforts down. To mitigate this, we recommend that any new requirement or standard is based on principle rather than process.

Overall, we recommend that government acknowledge both existing regulatory drivers and industry practices before introducing cross-cutting or overlapping requirements to report against new standards. As the discussion document recognises "…any increase in regulatory burden will result in increased costs for end-users, increased costs for government, and/or lower quality services". The price quality regime in principle recognises the link between meeting quality standards and making investments. There is a risk that new standards would not result in better resilience outcomes if they were not also supported by the right funding. In the case of regulated electricity networks, a key input here is the Commission's price-quality pathway.

Vector's key points

1. Many critical infrastructure entities already have rigorous risk assessment, management and reporting requirements in place. The approach of government should be to support and enable best practice, and, to target any additional requirements towards gaps in performance and regulations

Vector already implements a rigorous risk assessment process which feeds into internal and external reporting. In addition to the Board Risk Audit Committee (BRAC) Vector implements a cross-functional network security strategy which draws on global best practice including the International Energy Agency (IEA) Electricity Security Framework. Vector's network security strategy considers the dimensions of network security as: reliability, resilience, and adequacy.



Source: IEA Electricity Security

A key challenge to this strategy is the failure of the Commerce Commission's price quality regime to fund or incentivise resilience. In fact – by excluding High Impact, Low Probability Events (HILP) events from the reliability framework, the quality regime implemented by the Commerce Commission leaves the ability of regulated networks to respond to an emergency expressly out of scope.

Reflecting the new threat environment presented by digitalisation and cyber security recognised by the DPMC, Vector has also been proactive in developing the world leading cyber security solution – *Equalize* – by drawing on global expertise and capability. Vector is now making this solution available to the wider sector, adding to the significant coordination and information sharing which already occurs across the sector to strengthen our collective resilience. In this context, we think any additional steps to increase information sharing between critical infrastructure entities – and between critical infrastructure entities and government – should be based on partnership. We remain opposed to enhanced information gathering and sharing powers for NEMA as part of the Emergency Management Bill, which the DPMC refers to. We also note the beneficial ownership register, referred by the DPMC, is an example of an intervention which seems out of place in the regulated distribution sector – whereby many networks are majority owned by community trusts on behalf of consumers.

Details of our ownership, approach to climate resilience, risk management, emergency response, and cyber security, is already disclosed publicly across our ten-year Asset Management Plan (AMP) which we are already required by the Information Disclosure regime to publicly disclose, and our Annual Report. We attach our 2023 AMP as Annex 1 to this submission and recommend that the DPMC focus on the following sections:

1.7 Climate resilience – pg 9
6.3 Risk Management – pg 45
6.4 Event Management and Emergency response – pg 48
6.8 Cyber Security – pg 53

We also attach our Annual Report as Annex 2 and our response to the Task-force on Climate-related Financial Disclosures (TCFD) regime as Annex 3. The TCFD response to XRB disclosure requirements sets out comprehensively our exposure to climate related financial risk – including that which stems from the physical effects of climate change.
Rather than seek to duplicate what critical infrastructure entities already have in place (e.g., new information sharing arrangements, or additional accountabilities for directors / senior leaders), we recommend that the DPMC channel its efforts to improve existing regulations to ensure they enable existing efforts to improve resilience.

2. There is a need for stronger alignment of the Commerce Commission price-quality regime to resilience. Although this regime funds regulated electricity networks, it does not directly fund resilience. New standards or obligations should not be implemented by way of a separate and new resilience regime as this would exacerbate the disconnect between investments needed and investments funded. Instead, our existing regime need to respond to the resilience challenges the DPMC highlights.

The existing price-quality regime of the Commerce Commission (the Commission) is intended to provide an indication of underlying reliability, normalised against major events. In doing so, this regime seeks to hold regulated networks to account for the quality of their services. However, as with the regulatory approach used by the Commission to determine allowable revenue, the quality regime is inherently backward looking – using past performance as a baseline for EDBs' future quality targets. The environment in which critical infrastructure entities must deliver security of supply has changed significantly from when this approach was developed – reflecting both the physical effects of climate change, an increasingly digitalised operating environment, and, a shift in customer expectations. Whilst the quality regime is intended to be normalised against major events – by treating them as outliers – we question if this is appropriate in an environment where extreme weather events are increasingly frequent. In this context there is a need for stronger consideration of the wider goal of resilience (not just reliability), which is not currently captured – or appropriately funded – by the price-quality regime.

The risk environment of 2023 – in which we are already experiencing a higher number of extreme weather events, resulting in greater unplanned outages – as well as the increasing risk of cyber-attacks – needs to be reflected in the price-quality regime. In the case of cyber-attacks – Vector receives billions of attempted cyber breaches per month. As highlighted by the discussion document "attacks are increasingly motivated by factors other than financial gain, for example, many cyber-attacks are geopolitically motivated and linked to nation state actors, who seek to disrupt essential services".

However, in the last default price pathway (DPP3) which sets out allowable revenue for a five-year period, no new funding was allocated to regulated networks for cyber security by the Commerce Commission. Similarly, a lack of funding was allocated for networks to keep spare parts in stock to enable efficient network restoration following an extreme weather event or to support resilience in the case of supply chain disruption or uncertainty. Indeed, in 2017 the then Minister of Commerce and Consumer Affairs had to issue a Government Policy Statement instructing the Commerce Commission to fund such investments for Wellington Electricity following the increased risk of an earthquake or tsunami in Wellington following the Hurunui and Kaikōura earthquakes, as determined by GNS Science. The fact that a Minister needed to issue such a statement to the Commerce Commission specifically to align the price-quality regime to these funding needs for resilience shows that our current regulatory framework is not working for resilience. Overall, our price quality regime fails to fund resilience and is blind to new drivers which characterise our risk environment – both short term and systemic. In 2023 such drivers include climate change and digitalisation.

The Boston Consulting Group (BCG) report *The Future is Electric* finds $22 billion of investment is required in New Zealand's distribution sector in the next eight years. However, the price-quality regime was designed to achieve marginal efficiency gains in a steady state environment and is not conducive with the investment required for resilience of our critical infrastructure. By not recognising financeability as a foundational element of the electricity economic regulatory regime, the draft Input Methodologies (IMs) recently consulted on by the Commerce Commission, risk taking investment for resilience backwards. For example:

- By continuing to index an EDB's Regulated Asset Base (RAB) to inflation, the draft IMs backends cashflow. Whilst un-indexing the RAB would result in the same total recovery over time (i.e., would remain NPV neutral), this would bring the timing of available cashflow forward. The IMs will flow into the next default price pathway (DPP) which will determine allowable revenue for regulated networks for the next five years.
- The draft IMs propose reductions to the weighted average cost of capital (WACC) percentiles. The WACC impacts financeability by acting as a building block for the rate of regulated return – the money that a regulated network can earn on investments.
- An arbitrary 10% revenue increase limit, from the previous DPP, resulting in over $1.5 billion in unrecovered revenue being denied to the six largest EDBs by 2030 according to expert analysis commissioned as part of the current Input Methodologies Review by the Commerce Commission.

As we said in an open letter to the Commerce Commission, "The Commission is pairing the greatest investment challenge for electrification for 50 + years with the weakest financing plan". In regards to the DPMC's statement that: *many critical infrastructures…may not have to significantly increase their expenditure to meet any new requirements* – we challenge this as an appropriate starting assumption, particularly for critical infrastructure entities whose revenue is regulated.

Once again, we query whether a new reporting framework; resilience standard; critical infrastructure agency; or new government powers to intervene in an emergency, *are* the solutions to this potential funding shortfall and its impact on critical infrastructure resilience. Perhaps the solution is to align existing regulations to the work already being led by industry.

The role of the Commerce Commission in funding regulated electricity networks also presents a separate challenge to the DPMC's proposal to create a new regulatory regime. That is – that the activities (i.e., compliance) required by the new critical infrastructure agency / regime – are not funded by the separate price-quality regime of the Commerce Commission. As we said in response to the previous submission responding to the Civil Defence and Emergency Management Act reforms (which have since flowed into the Emergency Management Bill, currently at Select Committee):

EDBs non-exempt from Commerce Commission price-quality regulation will not have the costs associated with this work factored into their regulated revenue for the DPP period 2020-25.

While the proposal includes that the Relevant Sector Responsible Agency (for the energy sector - MBIE) must consider PELOS alongside other sector-relevant factors such as pricing and quality, it is the Commerce Commission, not MBIE, that determines these factors for the non-exempt EDBs.

We note that regulated energy providers already have regulatory commitments to the Commerce Commission and the Electricity Authority pertaining to service delivery expectations. These existing requirements should be considered carefully through the development and implementation of the PELOS requirement to avoid duplication, as well as to consider learnings from these existing arrangements.

Whilst the changes contemplated by the DPMC go much further than the changes advanced through the earlier consultation on changes to the Civil Defence and Emergency Management system and included in the Emergency Management Bill – the above points remain substantively relevant. We strongly oppose the creation of requirements from one regulatory regime and/or entity that are not supported by another.

As we discuss further it is also critical that market and technology regulatory settings are driven to the goal of accelerated digitalisation. Just as new technology integration comes with risks to resilience (as acknowledge by the DPMC), it also has a key role as part of the solution – if we are proactive in implementing the right settings today. Finally, there is a further "low hanging fruit" opportunity to increase resilience by progressing the review of the vegetation management regulations.

In sum, there is scope for our existing regulations to be better calibrated towards the goal of resilience – and there is a risk that the introduction of a new regulatory regime without this calibration will result in duplication or misalignment. This would not improve critical infrastructure resilience but would likely stymy progress. We appreciate the goal of the DPMC to take a systems' view in ensuring that the regulatory settings are right to drive the resilience of critical infrastructure in 2023 and beyond. We understand that supporting this strategic approach to our infrastructure is part of the role of Te Waihanga – the Infrastructure Commission. In any case, we urge the DPMC to adequately consider the role that existing regulations and entities have in our system before advancing a new regime and agency.

As we discuss further on page 15 we think that there is an opportunity to strengthen a whole-systems approach to our energy system more broadly through a Ministry for Energy. This is particularly to ensure a secure and reliable energy transition. The UK's Department of Energy Security and Net Zero recognises the need for a coordinated response to ensure energy security and reliability through our climate change response. We recommend such an entity is established in New Zealand by way of a Ministry for Energy to ensure system security and resilience by way of a coordinated approach to our energy transition – that understands the system as a system, and that takes account of the role of existing regulation.

3. There is a lack of clarity on what is meant by "national security risk" or what "government powers to intervene" could include exactly. In this context we oppose such a change as un-scoped powers for government intervention could obstruct the ability of a critical infrastructure entity to respond in an emergency.

We agree with the DPMC that:

"New Zealand faces a more complex geopolitical and national security environment than in recent history. The risk of foreign states – or proxies acting on their behalf – interfering in New Zealand's infrastructure system contrary to our national interests is higher than it has been in a generation and continues to grow. The critical infrastructure system is an attractive target for such interference. Espionage, sabotage and coercion can be – and is – attempted against the system regularly."

This is exactly why we moved early to develop *Equalize* – a leading cybers security solution leveraging global capability. As is revealed to us by *Equalize* we often experience over a billion attempted cyber breaches a month. Because we are not clear on what constitutes a 'national security risk' any new information sharing requirements could be impractical to implement and we oppose such new information sharing requirements as a result (i.e., which of these billion attempted breaches would fall in scope of the information sharing requirement?).

We also oppose the proposal to introduce new government powers to intervene in response to a significant national security threat. This is largely because the scope of such powers is not made clear, and we consider any unfettered government power to intervene could obstruct the ability of a critical infrastructure entity to respond in an emergency.

4. The role of technology to strengthen resilience has been underestimated by the DPMC. There are opportunities to take a more holistic view in building resilience which includes customer technologies and a more distributed system.

Whilst the discussion document acknowledges that "…the most resilient organisation is not necessarily the one with the 'hardiest' assets, but the one that can continue to deliver services to communities most consistently" it has also underestimated the role of non-traditional technologies to enable the continuity of services in an emergency.

For electricity networks, the use of non-traditional solutions such as distributed energy resources (DER) or micro-grids – as well as digital demand response technologies – can play a key role in improving system security and resilience. DER can reduce communities' reliance on a single point of failure, providing alternative sources of energy in an outage. This can reduce the risk of a community being 'cut off' from power supply, even when the grid or network has been compromised. There are structural barriers in our market regulation framework however for regulated networks to invest in such solutions. Provisions concerning a regulated networks involvement with connected renewable generation for instance, have been transferred from primary legislation to The Electricity Industry Participation Code. The criteria for investment in distributed generation has proven a barrier for networks across NZ already. These provisions are part of a wider market-regulatory approach – of seeking to silo parts of our electricity supply chain. However, by seeking to restrict network involvement in connected generation this approach is at odds with the goal of increasing investment in localised renewable generation, despite the role that this could play in driving greater resilience.

In addition to distribution generation, DER more broadly, presents an opportunity to reduce avoidable outages by strengthening system security. For example, by acting as sources of connected capacity, EVs could help to stabilise the system in a grid emergency – much like how hot water load control was used for load shedding to avoid outages in Auckland during the August 9th grid emergency.

As highlighted by the Ministry of Business Innovation and Employment's (MBIE) Investigation into electricity supply interruptions of 9 August:

"The increasing use of EVs will either be part of the solution or contribute to the problem. We can avoid unnecessary future increases in peak demand if EV charging is managed to shift load…While the demand side's discretionary load was put to good use in the 9 August event, it was underexploited. It could have saved the day entirely. It ought to have been fully exploited, as the available supply side was. We propose that in future the demand side's discretionary load be accorded attention equivalent to the supply side."

We agree.

The potential use of EVs for system security however depends on the right market regulation and technology settings. EV chargers must have 'smart' capability (an IP address) so that they can be remotely managed. We support proposals to widen the remit of EECA to implement a regulated standard to ensure that EV chargers installed in New Zealand have this capability.

In addition to EV chargers being smart, there also needs to be aggregators or DER managers who are playing a role in managing them. We support the creation of flexibility markets whereby demand response aggregators are offering DER management services for the purpose of system optimisation for lower costs to consumers. This creation of flexibility markets should be accompanied by provisions to enable a network to manage distributed assets for the purposes of system stability in an emergency. As above this requires regulated networks to have greater involvement with non-traditional technologies than what was contemplated by our 1990s market regulatory framework. The alternative is an over-reliance on traditional solutions which will reduce utilisation, increasing costs, and which will fail to realise the potential – or protect against the risks – of digitalisation.

In addition to the opportunity to recruit customer technologies for greater system security, these distributed assets can also support greater resilience by offering customers access to alternative power sources. As above, network involvement in such customer assets however is effectively prohibited by our market regulation despite the role that this could play in driving resilience efficiently – particularly in remote parts of the network where traditional network investments would be largely underutilised. Consumers would still have to pay for such underutilised traditional network infrastructure in their electricity bills for decades to come.

The use of distributed back-up generation may be particularly valuable for commercial customers – especially if they are themselves critical infrastructure entities. We note for example, an opportunity for telecommunications providers to have more distributed backup generation at their disposal in an emergency. We also note that in the case of supermarkets – some had access to back-up generation during Cyclone Gabrielle and others didn't. Whilst these choices are currently at the commercial discretion of these entities, we appreciate that an improved and more comprehensive definition of 'critical infrastructure entity' with the Emergency Management Bill (and the broadening of existing responsibilities under the Civil Defence and Emergency Management regime) will result in stronger obligations for such entities to have greater contingencies in place. However, we do consider this is also an example of the impact that non-traditional technologies can have to resilience and the value in taking a broad view of resilience-solutions that can support

better outcomes for New Zealanders. This is particularly important given the interdependencies between critical infrastructure entities.

Florida provides a case study of where a broader understanding of resilience and the role of non-traditional or distributed solutions serves community resilience well in an emergency. In 2022 Hurricane Ian resulted in outages for millions of customers in the state. However, microgrids (distributed generation systems) ensured continued access to electricity in at least three residential communities, retail establishments, medical facilities, a university and manufacturing operations across the affected states of Florida, Georgia, Virginia and the Carolinas. The role of DER in an emergency had been explored by the United States Department of Energy (DOE)[1] and we encourage the DPMC to do the same. This also signals the value of a dedicated Energy Ministry to similarly identify and enable the realisation of such solutions.

5. Critical infrastructure entities are not 'one-size fits all' and minimum resilience standards will not by themselves drive resilience

Natural disasters have unforeseen consequences and imposing a set standard across different critical infrastructure entities for a range of disasters is unlikely to result in the advancement of solutions that are the best fit for New Zealanders in emergency circumstances. In 2019 Christchurch airport partially lost power causing a radar surveillance outage for 47 minutes. The outage was initiated when a capacitor exploded in an uninterruptible power supply unit in the Christchurch air traffic management centre. The Transport Accident Investigation Commission found this failure alone should not have caused the service loss. Correct wiring between the uninterruptible power supply unit and the core digital network equipment and greater access to back-up generation could have resulted in a more resilient outcome – but we are unclear how a set standard which seeks to cover all critical infrastructure in all emergencies could have achieved this given the technical dependencies across the airport's own technologies and between critical infrastructure entities. For this reason we oppose the implementation of a resilience standard which seeks to cover all infrastructure – and suggest that in case any such requirements are developed, they focus on principle rather than process.

The approach contemplated by the DPMC – of assessing asset criticality / significance and tailoring a risk-mitigation response – reflects best practice asset management which is already happening across critical infrastructure entities and which is tailored to critical infrastructure entities' own assets. Vector's network security strategy includes a vulnerability assessment approach of: creating an impacts framework using inputs from key stakeholders; implementing a vulnerability assessment methodology; identifying climate hazards and their impacts; identifying potential vulnerabilities; associating hazards and vulnerabilities; calculating likelihood of hazards and consequence of vulnerabilities; and creating a final score to align against a risk matrix for mitigation. Because this is already happening across critical infrastructure, rather than implement new requirements on the basis of a critical infrastructure entities' significance or criticality, we recommend that instead the DPMC undertake a gap analysis of performance and instead tailor the stringency of any new requirements to performance. Similarly, in regards to information sharing

[1] https://www.energy.gov/sites/prod/files/2019/09/f66/distributed-energy-resilience-public-buildings.pdf

arrangements – we recommend that the DPMC leverage the existing TCFD framework, including the potential expansion of this existing regime to include critical infrastructure entities which are currently out of scope.

1. Section 1: Background and context

1.1 The paper discussed four megatrends: i) climate change, ii) a more complex geopolitical and national security environment, iii) economic fragmentation, and iv) the advent and rapid uptake of new technologies. Do you think these pose significant threats to infrastructure resilience?

We agree that these four megatrends pose significant threats to infrastructure resilience. We agree with the discission document's commentary on the potential risk associated with the advent and rapid uptake of new technologies. However, as we stated above, new technologies are also part of the solution.

We agree that digitalisation of our electricity system will increase the 'surface area' of potential cyber-attacks, and that the integration of IT and OT systems presents new vulnerabilities and risk. However, the cyber security solution developed by Vector Technology Services (VTS) *Equalize* has been designed specifically to address these vulnerabilities, drawing on global capability, and is now available to networks across New Zealand to strengthen our sector's resilience.
Similarly, whilst the greater use of DER has the potential to challenge our traditional electricity supply chain by increasing complexity and demand on our electricity system (partnered with greater reliance on intermittent renewable supply) – there is an opportunity to leverage distributed solutions to drive improved rather than reduced security of supply. This rests on digitalisation and the alignment of our market regulatory framework to accelerate rather than hinder the integration of digital technologies.

The key to unlocking this opportunity is to proactively accelerate the integration of enabling technologies through the right market and technology settings. This requires regulation that is orientated towards the challenges and opportunities of the future – rather than those of the past. We will not achieve the change required through regulatory incrementalism or path dependency – nor through an additional resilience regulatory regime which does not recognise the role of these existing settings.

2. Section 2: Potential barriers to infrastructure resilience

2.1 If you are a critical infrastructure owner or operator, what additional information do you think would best support you to improve your resilience?

We support the provision of climate forecast data and are strongly supportive of the work of the National Institute of Water and Atmospheric research (NIWA) to date. Vector has already worked with industry partners to undertake scenario modelling aligning the IPCC scenarios of RCP 4.5 and

RCP 8.5 with the Network for Greening the Financial System (NGFS) standards. RCP4.5 aligns with “orderly” and ‘disorderly’ scenarios – with RCP8.5 aligning with ‘hothouse’ (the counterfactual reflecting no policy mitigation to climate change). This analysis forms the basis of our TCFD disclosures.

We note that the XRB is also encouraging the development of sector wide modelling to inform the TCFD reporting of energy sector participants. The timing proposed for release of NIWA modelling of IPCC scenarios (which the National Adaptation Plan proposed for June 2024) would be too late for TCFD disclosures to incorporate this modelling in that year.

We still support the provision of this data and the work of NIWA. We strongly recommend that when this data is released the details of the model is made public. It is important that industry can see the input variables used and the output variables that result, in granular detail. This is best practice in the interests of transparency. To inform this work we recommend a strong focus on cyclonic events and resourcing needed to undertake this analysis.

In addition to this we support access to short term data and forecasting such as better rain radars; improved weather forecasting; easier utility access to more detailed data/forecasting and local government data such as flood maps, geology reports, contaminated ground, LiDAR and aerial mapping.

However, the future will likely require a hybrid approach to the data that critical infrastructure entities use for resilience planning – rather than relying on one data source. This would include both national publicly available data, as well as further bespoke information, such as asset level risk assessments conducted by critical infrastructure entities. It is therefore critical that the Commerce Commission allows companies like Vector to have an opex-uplift to conduct such analysis to better plan asset infrastructure, which in turn will improve resilience.

Whilst it may be out of scope of this NIWA modelling we also recommend that the impact of consumer behaviours be considered carefully as government and industry develop modelling and analysis to inform our resilience planning. Behaviours will be an important – and changing – variable for the physical effects of climate change. Consumer preference is also a critical consideration in shaping adaptation policies and ultimately ensuring their fairness and effectiveness.

Having access to data on the location of DER (including EV chargers) when it is installed would also be useful in providing visibility of these assets to support better planning and emergency management. We have consequently made several recommendations to the EA to achieve this – including an expansion of the existing ICP registry (DER registry) to include the size and type(s) of DER found at each ICP. We would appreciate the support of the DPMC in advocating for this.
There is a further opportunity to improve distribution system resilience through improved access to Network Operations Data Sets (NODS) from residential smart meters. Network operators have limited visibility into the performance of the low voltage components of their network. By having improved access to smart meter data, network operators can design and operate more efficient

and resilient low voltage networks, and by having better access to this data in real-time they can use it to greatly improve their operational response during an event.

I. Access to the complete network's smart meter NODS data provides a comprehensive view of the operating performance of the distribution system from the customer's perspective. It can be used to greatly improve visibility of the low voltage (LV) network which promotes greater resilience through improved LV network performance monitoring, more precise network modelling, and proactive network balancing. It also supports improved precision and accuracy of customer connectivity information which supports improved customer communications, active safety monitoring and improved service level monitoring.
II. Better access to smart meter data delivered to the distributer in real-time allows greatly improved situational awareness of the network during events. Primarily supporting customer safety monitoring and highly accurate customer outage monitoring.

2.2 What do you think the government should do to enable greater information sharing with and between critical infrastructure owners and operators?

We oppose new information sharing requirements. As we mentioned, the existing reporting obligations for regulated networks are already great.

The discussion document references reforms underway to enhance information gathering and sharing powers for the National Emergency Management Agency (NEMA). These reforms are captured in the recently introduced Emergency Management Bill – which will replace the Civil Defence Emergency Management Act 2002. As we said in a submission responding to earlier work to consult on these reforms, we oppose the proposed new requirements for reporting, monitoring and evaluation of critical infrastructure entities.

This is because we are concerned about: the disclosure of critical or sensitive locations if this was not managed securely; ensuring that such information requirements did not impose an unnecessary burden on the sector; and, ensuring that such new requirements actually contribute additional value in improving critical infrastructure security and reliability. The first two of these points have been acknowledged in the discussion document. We appreciate the recognition of the potential for changes to result in unintended risk and cost and the intention to avoid this. In our earlier submission we said:

As we mentioned in our submission responding to this proposal in July [2021] we do not agree that specific/sensitive critical infrastructure information relating to service levels (e.g., restoration times for particular parts of the network) that can be shared with other Critical Infrastructure Entities and the sector responsible agency, should be placed in the public domain. This is because if this information gets into the wrong hands, it could be used to create a blueprint of high impact areas of the electricity or gas network that would require long restoration times. This information is popular with hackers and anyone wanting to cause harm or fear to the community… The requirement on CI Entities to establish and update PELOS on a triennial basis will impose a non-trivial burden on the sector.

There is also a risk that the introduction of new information sharing requirements would drive an uplift in reporting and monitoring capabilities, which would not by itself improve resilience.
We will submit on the Emergency Management Bill directly and separately – however we note considerable overlap between the below objectives in the Bill's General Policy Statement, and the objectives proposed in this discussion document – particularly to establish new minimum standards for critical infrastructure entity resilience; to increase reporting and monitoring requirements; and to re-enforce accountability of critical infrastructure providers.

The Bill proposes to improve the resilience of New Zealand's infrastructure and infrastructure services before, during, and after an emergency by—

- *requiring critical infrastructure entities to proactively, and on request, share information with the National Emergency Management Agency (**NEMA**), regulatory agencies, and Emergency Management Committees for monitoring and planning:*
- *requiring critical infrastructure entities to establish and publish their planning emergency levels of service:*
- *requiring annual reporting to the Director of Emergency Management, and the critical infrastructure entity's responsible agency.*
  - *Emergency Management Bill – General Policy Statement*

We do question how robust the sequencing of this policy work is – with the DPMC discussion document consulting on proposals that have in part already been introduced to the House as legislation by way of the Emergency Management Bill. We also note that this strategy is being advanced without an understanding of the effectiveness of the proposals in the Bill to address many of the concerns expressed by the DPMC. Once again, we recommend that new interventions are preceded by a gap analysis and advanced on the basis of additionality. We can't see how this could be possible when the interventions proposed in the Emergency Management Bill have not yet been implemented – and their effectiveness or adequacy not yet assessed.

In the case of new information sharing requirements our view is that the sector is already coordinated and shares information effectively to improve resilience. In particular, a number of existing forums for sharing cyber-related information currently exist (CSSIE, NZITF, the NZ ICS Cyber-Technical Network, and CIO Leadership Forums). These forums are driven by relationships across the sector and a desire to improve situational awareness and cyber-preparedness. This sector-led approach provides a formal structure for regular engagement.

We do not see a need for new information sharing requirements – however, if such interventions are advanced we advocate for these being introduced incrementally and not subject to audit requirements to help reduce the compliance burden to critical infrastructure entities

2.3 Would you support the government being able to set, and enforce, minimum resilience standards across the entire infrastructure system? If so:
– what type of standard would you support (e.g. requirement to adhere to a specific process or satisfy a set of principles)?

We oppose this. This is because the operational realities faced by different critical infrastructure entities are complex and varied. Our engagement with government during Covid-19 highlighted how important it is that we are working closely with government in responding to emergencies. It also revealed gaps in policy understanding of some operational risk dynamics – for example, supply chain resilience.

We said the below in response to the proposed Planned Emergency Levels of Services (PELOS) regime, which has now been advanced through the Emergency Management Bill. Whilst we understand that the DPMC is considering minimum resilience standards which go beyond the PELOS regime, we believe that many of these points remain relevant to any new resilience standard and so we reiterate them here:

It is not clear to us how a review of CI Entities' systems and processes would be standardised across the sector given the different roles of CI Entities in the energy sector. We consider this would be impractical (if not impossible). This potentially raises several questions, e.g. what standards are we being measured against, what is considered a timely response, how many customers could be impacted, what are the potential damages, etc.

We consider that the development and implementation of process-based requirements for critical infrastructure entities would require an uplift in government policy capability in technical areas and would add little or no value.

If any new standard was implemented, it should be principle rather than process-based – and targeted to critical infrastructure entities on the basis of performance, and whether or not there is existing regulation. To achieve this we recommend that the government undertake a gap analysis of both critical infrastructure processes and performance, and existing regulations, and target any new requirements towards these gaps – rather than on the basis of infrastructure criticality or significance as the discussion document considers (which would almost by definition duplicate regulations).

We are pleased to see that the discussion document recognises existing regulatory regimes – including the price-quality regime administered by the Commission – and the interaction of any new resilience standard. We provide some further information about this and other existing regulations which can have a key impact in improving resilience outcomes – if they are directed as such right now.

<u>Price-quality regime</u>
This price quality regime regulates the allowable revenue of regulated electricity distribution businesses (EDBs), as well as quality standards – by setting out allowable outages measured by

duration (SAIDI) and frequency (SAIFI). This regime, in principle, captures a balance between price and quality – recognising that the revenue that is available for investment in infrastructure can strengthen quality outcomes. We agree with the discussion document however that: "Increasing New Zealand's annual investment in high-quality critical infrastructure resilience should save money in the long term". We also note that the price quality regime is designed to avoid the degradation of reliability – whereas the goal of the DPMC is orientated towards both reliability and resilience.

Resilience is wider than reliability – and is focused not just on avoiding the unplanned network outage, but, how our infrastructure responds in emergencies or extreme weather events. Our view is that the price quality regime (including both SAIDI/SAIFI and the approach to funding) was not designed for our 2023 and future risk environment.

However, for regulated electricity networks – ensuring that our sector's funding regime is aligned with the demands imposed by the physical effects of climate change; increased risk of cyber-attack; and increased customer expectations and reliance on electricity – is a critical first step.
We have recently responded to the Commission's draft Input Methodologies (IMs Review). The IMs review will flow into the price pathway set early next year, determining the available revenue for regulated networks. This will have a material impact on their investment profile for the next five years. Our recommendation is that the Commission explicitly take into account the impact of climate change and recognise financeability as a core element of the framework. This is to ensure that the investment allowed is in step with what is required to respond to our current risk environment and enable our energy transition.

We recommend that government turn its attention to this framework with urgency – and that this is prioritised before the implementation of a duplicative set of resilience standards or reporting requirements for regulated electricity networks.

<u>Vegetation management regulation:</u>

Another example of a regulatory enabler which could support greater resilience is the *Electricity (Hazards from Trees) Regulations 2003.* In extreme weather events up to 70% of outages on our network are caused by vegetation (during the April 2018 storms this was around 70% whereas for Cyclone Gabrielle this was ~60%). Of vegetation related outages approximately 80% are caused by trees which are outside the scope of regulations – and the zone within which EDBs can manage them ("out of zone" trees). The impact of out of zone trees in driving outages is consistent across extreme events and EDBs. A review undertaken by the Electricity Network Association (ENA) the *Electricity Distribution Sector Cyclone Gabrielle Review* identified out-of-zone trees as the largest cause of outages for EDBs. This means that the regulation does not engage risk. We therefore urge the review of the *Electricity (Hazards from Trees) Regulations 2003* to be progressed with urgency. Consultation on this closed in May and we have not heard an update on progress.

Other considerations:

The ENA report into the sector's response to Cyclone Gabrielle also highlighted the skills shortage as a key constraint in restoring power to communities. Overall increasing and targeting the development of technical skills in New Zealand's energy sector should be a critical priority.

"Impacted EDBs expanded the number of people involved in the response. However, due to the scale of Cyclone Gabrielle (which was difficult to anticipate in advance), the ability to expand was constrained by the number of trained people within the EDBs (this being more acute in the smaller EDBs). EDBs experienced varying constraints across the restoration process (from outage notification, network control, dispatch, logistics and field work). The extent of the impact across the North Island and roading failures in affected regions severely limited the level of mutual aid that could be provided in the initial stages of the cyclone. However, despite the access challenges, mutual aid was provided as the event progressed, and this included field resources and network controllers".

- *Electricity Distribution Sector Cyclone Gabrielle Review 2023*

2.4 Would you support the government investing in a model to assess the significance of a critical infrastructure asset is, and using that as the basis for imposing more stringent resilience requirements? If so:
– what options would you like the government to consider for delivering on this objective?
– what criteria would you use to determine a critical infrastructure asset's importance?

Methodologies to assess the significance of infrastructure asset criticality to inform more stringent resilience requirements is already integrated as part of good asset management practice across critical infrastructure entities.

Indeed, the *Electricity Distribution Sector Cyclone Gabrielle Review* found that practices to identify risks were generally robust.

> *Our assessment indicated that hazard identification is generally robust for typical hazards (snow, tsunami, volcanic activity, wind), but work is at an earlier stage in relation to flooding, geotechnical hazards, and assessing how hazards may alter with climate change. The latter three issues have emerged more recently due to recent weather trends. Identifying assets vulnerable to hazards and preparing mitigation plans is also generally robust for typical hazards but still forming for flooding and geotechnical hazards".*

We are concerned about the scope for duplicating or misaligned requirements which would not improve resilience. In some cases the most critical infrastructure entities are also those with the greatest existing regulatory burden. Therefore, deciding whether or not to implement more stringent resilience requirements on the basis of an asset's importance is almost by definition biased towards duplication.

2.5 Do you think there is a need for the government to have greater powers to provide direction or intervene in the management of significant national security threats against a critical infrastructure? If so:
– what type of powers should the government consider?
– what protections would you like to see around the use of such powers to ensure that they were only used as a last resort, where necessary?

We are not clear on what is meant by: *"greater powers to provide direction or intervene in the management of significant national security threats against a critical infrastructure"* exactly. However we do not believe that such new powers are likely to result in a material difference to resilience and consider there are stronger opportunities for the government to align existing regulations to support the work to protect infrastructure against national security threats which is already underway.

We understand and support the intention for government security agencies to be working more closely with critical infrastructure entities in mitigating and responding to risks. We agree with the discussion document that partnership is a key principle that should underpin any interaction here. We recommend that efforts are made to strengthen this engagement and build mutual understanding as a first step in strengthening this coordination. This can provide a clearer view around what formal requirements can add the most value before these are designed and implemented.

2.6 Do you think that there is a need for a government agency or agencies to have clear responsibility for the resilience of New Zealand's critical infrastructure system? If so:
– do you consider that new regulatory functions should be the responsibility of separate agencies, or a single agency?
– do you consider that an existing entity should assume these functions or that they should be vested in a new entity?
– how do you see the role of a potential system regulator relative to sectoral regulators?

As we have described throughout this submission, the electricity distribution sector is already heavily regulated by multiple regulators. In this context, the risk of creating a new agency to enforce a set of standards and requirements, is that such activities would not be funded by the Commerce Commission's price-quality framework. Indeed, navigating the jurisdictions of both the Commerce Commission and the Electricity Authority in our operating environment is already complex, resource intensive, and characterised by overlapping and misaligned requirements. We also query the need for a new critical infrastructure agency given the role of Te Waihanga, the Infrastructure Commission.

We support the goal of driving greater coordination across government to deliver the outcomes required of our critical infrastructure in 2023 and beyond. Whilst we believe that a new critical infrastructure agency would take progress towards this goal backwards, we do recommend a

Ministry for Energy. This can drive needed coordination between the many different entities and workstreams across government that have a role in delivering a secure and reliable energy transition. This is also a crucial opportunity to ensure that our regulatory frameworks are aligned with government policy goals. We have provided examples of where we do not believe that this is currently the case.

2.7 Do you think that there is a need for compliance and enforcement mechanisms (e.g., mandatory reporting, penalties or offences) to ensure that critical infrastructure operators are meeting potential minimum standards? If so:
– do you consider that legal obligations should be applied to the entity, to the entity's directors/executive leadership, or a mix of the two?

Overall the burden on critical infrastructure entities to deliver resilient outcomes is already high and formalised in requirements for critical infrastructure entities to comply with their obligations in the Civil Defence and Emergency Management Act. As pointed out by the National Adaptation Plan (NAP) consulted on last year, there are existing workstreams to improve reporting around the impacts of climate change – such climate related disclosure requirements under the Task-force on Climate-related Financial Disclosures (TCFD) workstream. We recommend that the DPMC consider utilising this existing framework and its significant reporting requirements –(including an expansion to include unlisted critical infrastructure entities) before new reporting requirements are created. As we said in our submission responding to the NAP, resilience planning must be integrated into BAU asset management and planning. As such steps to increase reporting or resilience planning should draw closely on existing frameworks.

We believe that where the government can add value is through the alignment of regulations and funding levers – in many cases, existing regulations and funding levers. Given the regulatory environment for regulated electricity networks this must include consideration of our existing market and economic regulatory regimes.