19 April 2026

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

Submission via parliament submission portal

Dear Group Secretariat,

Submission on Enhancing the cyber security of New Zealand's critical infrastructure system

Introduction

Electricity Networks Aotearoa (ENA) appreciates the opportunity to make a submission on the discussion document *Enhancing the cyber security of New Zealand's critical infrastructure system*.

ENA is the industry membership body that represents the 29 electricity distribution businesses (EDBs) that take power from the national grid and deliver it to homes and businesses (our members are listed in Appendix A).

EDBs employ over 7,800 people, deliver energy to more than two million homes and businesses, and have spent or invested $6.2 billion in network assets over the last five years. ENA harnesses members' collective expertise to promote safe, reliable, and affordable power for our members' customers.

Electricity distribution networks are a core component of New Zealand's critical infrastructure system. As the discussion document recognises, infrastructure such as electricity networks underpins economic activity, public services, and community wellbeing, and is increasingly exposed to evolving cyber security risks.

Role of EDBs in critical infrastructure and cyber security

EDBs operate essential infrastructure that enables the functioning of other critical sectors, including health, transport, communications, and financial services. Disruption to electricity distribution can have cascading impacts across the wider economy and society.

EDBs already treat cyber security as a core operational and governance risk. Cyber risk is actively managed at a Board level.

Over recent years, EDBs have increased collaboration on cyber security, including sharing threat information and aligning practices across parts of the sector. Mechanisms such as and sector-led communication channels support voluntary information sharing about threats.

Many EDBs are also progressing toward adoption of the Australian Energy Sector Cyber Security Framework (AESCSF).

Overall position on proposals

ENA supports the intent of the ideas and proposals in the document to improve the cyber resilience of New Zealand's critical infrastructure system.

ENA supports, in principle:

- Improved information sharing between government and infrastructure providers·
- A clearer understanding of critical infrastructure and interdependencies
- A proportionate uplift in cyber risk management practices

However, any regime must carefully consider affordability and the ability of EDBs to fund compliance. Costs will ultimately be borne by consumers, in an environment where electricity prices are already increasing. For smaller EDBs, costs are spread across fewer consumers, resulting in disproportionately higher impacts. This reinforces the need for a proportionate, risk-based approach.

Legislative and reporting framework for 'critical infrastructure' should consider broader roles and responsibilities for infrastructure service providers (e.g. asset resilience requirements, emergency response etc, place within new resource management legislation). Duplication, misalignment, and/or uncertainty of roles and responsibilities can increase risk of non-compliance and increase compliance costs.

Scope, definitions, and system design

ENA notes that the discussion document defines critical infrastructure in multiple ways—sometimes referring to the provider, and at other times to the infrastructure itself. Greater clarity is required to ensure that obligations apply appropriately to the components that deliver essential services, rather than uniformly to entire organisations.

The concept of "critical components" is useful and should be consistently applied across measures, not limited to risk management requirements.

Supply chain considerations

ENA supports inclusion of key suppliers within scope, recognising cyber risk is often introduced via third parties. However, clearer guidance is needed on:

- which suppliers are in scope (e.g. OT vendors, MSPs, cloud providers)
- when obligations are triggered

Many suppliers are offshore and outside jurisdiction. Obligations should therefore be based on reasonable endeavours and risk-based controls, not strict liability.

The regime should:

- recognise existing certifications and avoid duplication
- apply proportional requirements for smaller suppliers
- provide practical tools such as model contract clauses and minimum expectations

Existing regulatory environment

ENA strongly encourages DPMC to engage closely with the Commerce Commission (the Commission) who we understand are currently developing an infrastructure resilience framework. The framework from the DPMC and the Commission must align to drive the best outcomes from this work. This includes the outcome of keeping costs to consumers as low as possible.

Government role and enablers

Government should support implementation through:

- New Zealand-specific guidance (especially for OT environments)
- Trusted information sharing platforms (e.g. ISAC-style)
- Central stewardship of sensitive datasets where appropriate

Integrated business structures

Some EDBs operate within wider organisations where critical systems (e.g. identity, cloud, networks, security tooling) are shared across regulated and non-regulated business units.

As a result, cyber controls cannot always be isolated to the regulated entity and governance, monitoring, and incident response operate at enterprise level.

Compliance will therefore:

- extend beyond the regulated EDB component
- increase costs across the wider organisation
- introduce implementation complexity

The regime should recognise this reality and allow pragmatic, risk-based implementation approaches. Clarity on cost recovery in regulatory settings will also be important.

Key consultation questions

1 Do you think the example thresholds for defining critical infrastructure have been set appropriately?

ENA considers that the proposed threshold of greater than 25,000 installation control points (ICPs) for electricity distribution businesses is a reasonable starting point for identifying larger electricity networks within the critical infrastructure system. However, ENA notes that thresholds based solely on size do not fully capture the criticality of electricity distribution infrastructure.

In particular:

- Smaller EDBs may supply electricity to critical customers, such as hospitals, emergency services, and key community infrastructure
- The consequences of disruption are not always correlated with network size
- Electricity distribution networks, regardless of size, play an essential role in enabling other critical services

ENA therefore considers that the proposed threshold is appropriate as an initial filter, but it should be complemented by a risk-based or consequence-based overlay, including the Minister's ability to designate critical infrastructure where warranted. This combined approach would provide greater confidence that infrastructure which is critical in practice is not inadvertently excluded from the regime.

ENA notes that the discussion document highlights that imposing requirements on all EDBs could exacerbate affordability pressures where costs are recovered across relatively small customer bases. While this is an important consideration, it is also critical that consumers supplied by smaller EDBs are not disadvantaged in terms of infrastructure resilience. All consumers should benefit from an appropriate level of resilience to cyber and other risks. Poor quality or less resilient infrastructure can exacerbate existing inequalities and increase costs for vulnerable communities.

ENA therefore encourages DPMC to consider both the affordability impacts of the regime and the potential consequences of underinvestment in resilience for these consumers. This includes identifying mechanisms to mitigate disproportionate impacts, such as a proportionate, low-cost baseline regime and potential support for smaller EDBs to achieve required cyber resilience outcomes.

ENA also notes that clarity is required on whether thresholds apply to infrastructure providers or specific infrastructure components, to ensure consistency in application.

2 Do you have any comment on the potential implications of each of the measures?

Measures 1–3 (information sharing)

These measures are broadly supported and align with current industry practice. They have the potential to improve system-wide awareness and coordination.

However, requirements must be targeted, and proportionate and existing voluntary mechanisms should be leveraged to inform what this measure looks like in practice.

For Measure 1 (government information collection), the benefits must clearly outweigh compliance burden. Greater clarity is needed on:

- how collected information will be used
- how value will be returned to industry (e.g. threat intelligence sharing)

For Measure 2 (voluntary exchange), ENA supports a voluntary model as proportionate. Government should play a stronger coordination role (e.g. via NCSC) to ensure equitable access and sector-wide benefit. Legal protections are also essential to ensure shared information is not used punitively or disclosed under the Official Information Act.

For Measure 3 (mandatory sharing), requirements must be clearly defined, secure, and appropriately protected.

Measure 4 (incident reporting)

ENA supports improved visibility of cyber incidents. However, the proposed 24-hour and 72-hour reporting timeframes may be challenging in practice.

Incident response and service restoration must remain the priority, particularly for critical infrastructure. Early-stage information is often incomplete and subject to legal review.

ENA recommends:

- a “reasonably practicable” standard (aligned with the Privacy Act)
- flexibility in early reporting
- clearer guidance on what constitutes a “significant incident”
- clarification of expectations for 24-hour vs 72-hour reporting

Safe harbour protections are essential to ensure good-faith reporting is not used punitively. A common reporting platform managed by the regulator would also improve consistency and efficiency and reduce duplication with existing regimes (e.g. Privacy Act). In addition to this, insurance implications should be considered to ensure reporting obligations do not unintentionally invalidate coverage.

Measure 5 (risk management programme)

ENA supports a baseline uplift in cyber risk management. However, requiring entities to "comply with" a framework will increase costs and administrative burden. It may not be achievable for all EDBs without unreasonable costs arising from compliance being passed through to customers. A requirement to align with frameworks would be more appropriate.

Requirements should:

- be outcomes-focused and flexible
- allow entities to adopt frameworks suited to their environment
- recognise hybrid and existing risk management systems
- avoid mandatory certification in the near term (given limited audit capacity)

The framework should also recognise maturity pathways and allow progressive uplift.

Cyber risk in electricity distribution involves unique challenges, particularly for operational technology, SCADA systems, and legacy infrastructure. Flexibility is critical to ensure practical implementation.

ENA also notes that the consultation material provides limited detail on how the proposed risk management programme is expected to evolve or be strengthened over time. This is likely to be the most cost- and resource-intensive component of the framework, and the area most at risk of becoming complex and costly if not carefully designed. Greater clarity on the intended scope, implementation expectations, and likely evolution of the programme would enable infrastructure providers to better assess impacts and plan investment. ENA therefore encourages DPMC to provide further detail in this area to support informed feedback and effective implementation.

Measure 6 (government direction powers)

ENA supports this measure in principle, recognising the government's access to some intelligence which EDBs will not have. However, use of this Minister power must be proportionate and well-justified. It should be required to be informed by expert agencies such as the National Cyber Security Centre and the Government Communications Security Bureau.

Additional safeguards should include:

- consultation requirements
- oversight mechanisms
- compensation provisions where appropriate

3 Are you able to quantify the potential cost of compliance with each of the measures?

ENA is not able to provide quantified cost estimates at this stage due to limited clarity on the specific requirements that will be mandated. However, ENA expects that compliance will involve both material capital investment and ongoing operational expenditure.

Likely cost drivers include:

- implementation or uplift of cyber security controls

- investment in new systems and technologies
- ongoing managed services, subscriptions, and support
- assurance, auditing, and testing requirements
- internal resourcing and governance capability

Costs may be significant, particularly for EDBs with lower existing cyber maturity. For regulated infrastructure providers, these costs are ultimately borne by consumers through pricing mechanisms.

ENA emphasises the importance of:

- a comprehensive cost-benefit analysis
- alignment with regulatory cycles (e.g. AMP, DPP)
- ensuring regulatory settings enable recovery of prudent cyber security investment

4 Do you support the risk management programme complying with an internationally recognised cyber security framework?

ENA supports the use of recognised cyber security frameworks. However, ENA does not support requiring strict compliance with such frameworks. Instead, ENA recommends a requirement to align with recognised frameworks and recognition of international sector-specific frameworks, such as the AESCSF. This approach reflects current industry practice and provides flexibility while still improving sector alignment. Alignment with frameworks also enables benchmarking of cyber maturity across comparable EDBs and improved consistency in risk management approaches.

5 Do you agree that penalties should apply to directors as well as to the organisation?

ENA agrees that cyber security is a governance-level responsibility. However, ENA does not support criminal liability for directors. Criminal liability is disproportionate to directors' control over operational risks and may deter qualified individuals from governance roles. It could also lead to overly risk-averse decision-making. Accountability should remain proportionate and primarily at the organisational level.

ENA also notes that monetary penalties imposed on EDBs ultimately reduce funds available for infrastructure investment and are passed on to consumers.

If director liability is pursued, consideration should be given to:

- guidance on director cyber security responsibilities
- statutory defences for reasonable steps
- phased implementation (e.g. 2–3 year transition period)
- director education and capability building

6 Do you think the thresholds for incident reporting are appropriate?

ENA considers that the proposed thresholds and timeframes for incident reporting are too rigid. In particular early reporting within 24 hours may not always be practical as resources will be prioritised toward response and recovery. Information may also be incomplete or inaccurate at early stages. ENA recommends a more flexible approach that specifically acknowledges these realities.

ENA notes that:

- early (24-hour) notification may be workable as an initial high-level alert
- further clarity is required on the content and expectations of a "full report within 72 hours"

A common reporting platform would improve efficiency and consistency. ENA also considers the proposed one-year transition period insufficient, given the scale of implementation required and limited availability of cyber expertise. A longer transition period should be considered.

Conclusion

ENA supports the intent of the discussion document to strengthen cyber security across New Zealand's critical infrastructure system. However, implementation will require careful design to ensure proportionality, regulatory alignment, and affordability.

Compliance costs are likely to be significant and must be balanced against the need to maintain investment in network resilience and service delivery. Continued engagement with the electricity distribution sector will be critical to developing a workable and effective framework.

Do not hesitate to get in touch with ENA if you would like to discuss any of the points raised in this submission. Please contact Sophie Tulley (sophie@electricity.org.nz) in the first instance.

Yours sincerely,

Sophie Tulley

Policy and Innovation Advisor

Electricity Networks Aotearoa

Appendix A: ENA Members

Electricity Networks Aotearoa makes this submission along with the support of its members, listed below.

- Alpine Energy
- Aurora Energy
- Buller Electricity
- Centralines
- Counties Energy
- Firstlight Network
- EA Networks
- Electra
- Electricity Invercargill
- Horizon Networks
- MainPower New Zealand
- Marlborough Lines
- Nelson Electricity
- Network Tasman
- Network Waitaki
- Northpower
- Orion New Zealand
- Powerco
- PowerNet (which manages The Power Company, Electricity Invercargill, OtagoNet and Lakeland Network)
- Scanpower
- The Lines Company
- Top Energy
- Unison Networks
- Vector
- Waipa Networks
- WEL Networks
- Wellington Electricity
- Westpower