19 April 2026

CONFIDENTIAL AND COMMERCIALLY SENSITIVE

By email: criticalinfrastructure@dpmc.govt.nz

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

Opening remarks

Meridian Energy welcomes the opportunity to comment on the government's discussion document *Enhancing the cyber security of New Zealand's critical infrastructure system.* We are pleased to see cyber security and digital resilience placed firmly at the forefront of New Zealand's critical infrastructure policy settings.

Meridian is Aotearoa's largest electricity generator, producing energy from 100 percent renewable sources – wind, water and sun. Our hydro stations produce enough electricity to power around 1.4 million homes each year and our wind farms generate enough electricity to power around 250,000 homes. Meridian is also a major nationwide electricity retailer through our Meridian and Powershop brands. We also own the Zero EV charging network, which is the second largest in the country, with 400 charge points installed and plans for more.

Meridian agrees that cyber risks to essential services are increasing in scale, sophistication and potential impact, and that these risks warrant a more coordinated and system-wide response. As an operator of critical electricity generation assets, Meridian recognises the importance of maintaining the security, reliability and resilience of infrastructure that New Zealanders depend on every day.

We support the Government's overall objective of strengthening the cyber resilience of critical infrastructure and acknowledge that current regulatory settings may not always drive a consistent or optimal level of cyber preparedness. In this light, Meridian considers it appropriate for the government to consider implementing a more structured framework, to

lift baseline capability, while also remaining proportionate, risk-based and aligned with international best practice.

Key themes in this submission

Meridian supports:

- Improved system-wide visibility of critical services, risks and dependencies
- Information sharing between government and critical infrastructure operators
- Clear and practicable cyber incident reporting obligations, and
- Minimum cyber risk management requirements that are outcomes-focused and risk-based.

Across the measures in the consultation, Meridian's consistent themes are:

- Clarity of definitions and thresholds
- Proportionality and scalability relative to asset criticality
- Strong protections for sensitive and commercially confidential information, and
- Where possible, alignment with existing regulatory obligations and sector practice.

Meridian also accepts that Ministerial powers may be appropriate for national security level cyber threats, provided that those powers are tightly scoped, used only in exceptional circumstances, and supported by clear safeguards, operational engagement protocols, and transparency.

Meridian also supports a graduated, risk-based compliance and enforcement model. Our view is that the regime should focus on capability uplift, clarity and consistency, rather than wide-ranging personal liability. We do not, for example, agree that personal liability for directors should form part of the regime. We consider that primary compliance duties should sit with the relevant critical infrastructure entities themselves. [1] The cyber security environment is extremely fast moving and is continuously evolving with new methods of attacking systems and technology emerging every day and the standards necessary to meet and respond to these challenges having to lift and improve at similar pace.. In this context, attaching personal criminal liability to directors is unlikely to drive better outcomes, and risks discouraging transparency, collaboration and continuous improvement.

[1] Meridian has reviewed the draft Institute of Directors submission and agrees with it.

One area that Meridian suggests should be considered in greater detail is how the proposed regulations will apply to third party service providers to critical infrastructure entities / the critical infrastructure sector, particularly to third party service providers of technology, digital and data services and operational technology services support, who may be providers to multiple critical infrastructure entities across New Zealand. To the extent any such providers are not observing adequate cyber security standards they have the potential to create systemic supply chain risk for the critical infrastructure sector. The regulations could leave it to critical infrastructure providers themselves to 'police' such parties but we suggest the critical infrastructure regulator should also have a role.

Meridian's approach to cyber security

Meridian already manages cyber security as a material operational and governance risk. This includes established oversight arrangements, continuous maturity uplift, and alignment with recognised frameworks such as the Australian Energy Sector Cyber Security Framework (AESCSF) and the National Institute of Standards and Technology Cyber Security Framework (NIST CSF).

On this basis, our feedback on the proposals is intended to be constructive and forward-looking, focused on how the measures can best achieve the intended outcomes. Meridian is supportive of the overall direction of travel set out in the consultation. Our comments have been developed with the aim of supporting a framework to enhance national resilience while recognising the operational realities of critical infrastructure entities.

Context and the reasons why this work is necessary

As the consultation notes, cyber threats to essential services are increasing in frequency, sophistication and impact. Disruption to critical infrastructure can have cascading economic, social and security effects. Meridian agrees that a more consistent, system-wide approach is justified.

Scope and definition of critical infrastructure

Meridian supports a principles-based definition of critical infrastructure, targeted at services whose disruption would materially impact communities or the economy. We support thresholds to ensure obligations focus on the most critical assets and services.

Based on the draft thresholds in the discussion document, our understanding is that electricity retailing is not explicitly captured as a critical infrastructure service. The communications and data section references managed and cloud services that are integral to the delivery of essential services by a critical infrastructure entity, but it is not clear whether this captures such services that support the supply of electricity to businesses and households. Meridian would welcome clarification on the intended treatment of electricity retailing and the supply of electricity at the retail level to households and businesses.

Meridian's feedback on the six proposed measures

Measure 1: allow government to collect specific information from critical infrastructure entities

Meridian supports this measure. We recognise that there is value in having system-level visibility of critical services and dependencies. As at least some of this information is likely to be commercially sensitive (lists of critical components, key dependencies and interdependencies), there should be strong protections around access, storage and use by the critical infrastructure regulator and Meridian notes and agrees with the protections referenced at page 13 of the consultation paper. Meridian also believes there is a crucial role to be played by government in picking up intelligence on cyber threats and where appropriate sharing that intelligence with critical infrastructure entities. In other words it is at least as important that information flows from government to critical infrastructure entities as it is for information to flow the other way.

Measure 2: establish a voluntary information exchange

Meridian supports the establishment of a formal information exchange. As noted above our view is that its effectiveness would be improved if information were to also be contributed by government. Reciprocal sharing of threat intelligence, vulnerability insights and relevant system-level information by government agencies is critical to the national interest.

Measure 3: require critical infrastructure entities to share certain information with each other

Meridian is supportive of measure 3, however there are practical and consequential points that need to be worked through relating to risk and confidentiality, and compliance with other laws and legal frameworks (e.g. competition law to the extent information shared is commercially sensitive, continuous disclosure rules under stock exchange listing rules and rules applicable to the wholesale electricity market, and potentially also privacy laws or restrictions on the sharing of confidential client information). This measure should also have clear thresholds in terms of both the timing of information sharing (whether this is at set times or event based, or both). The current framing of the measure is broad, with the intention to allow government to better understand interdependencies in the first instance, which suggests that this obligation might be expanded in future. As with our earlier comments, clarity as to intention and scope will ensure that entities are able to comply and government is able to get the right information.

Measure 4: require critical infrastructure entities to report cyber incidents

This is a particularly important area and Meridian is supportive of this measure. However, our view is that the reporting thresholds need to be appropriate and clear. Too low a threshold could result in high-volume, low-value reporting and obscure genuinely significant issues. The current definition of a "cyber incident", without any reference to materiality, is very broad. We are in principle comfortable with the 24 and 72 hour reporting timeframes.

Measure 5: require critical infrastructure entities to develop, implement and maintain a risk management programme aligned with an internationally recognised cyber security framework

Meridian is supportive of this requirement. We agree that a baseline obligation to identify critical assets, understand material cyber risks, and manage those risks systematically is essential to lifting resilience across the system.

Measure 5 will be most effective if it remains outcomes-focused and risk-based, rather than prescribing specific technical controls or solutions. Cyber risk is dynamic, and entities need a degree of flexibility to prioritise investments and controls in a way that reflects their assets, the current threat environment and their operating context.

We support the use of internationally recognised cyber security frameworks to support measure 5. We note that organisations do not typically "comply" with frameworks in a regulatory sense. Frameworks such as the NIST Cyber Security Framework and the AESCSF are used to guide, assess and mature cyber security practice over time. We

suggest the regime focuses on alignment with recognised frameworks, supported by justification and assurance, rather than treating frameworks as compliance instruments.

Meridian is concerned that, as drafted, the compliance aspects / requirements that accompany this provision appear to misunderstand the respective roles of Boards and Management of critical infrastructure entities. Meridian has reviewed a draft of the proposed submission by the Institute of Directors and Meridian agrees with it. Attaching responsibility for ensuring compliance to directors risks blurring the distinction between governance oversight and operational management in a regime that relies heavily on judgement-based concepts such as material risk and reasonable practicability. As already noted the cyber threat environment is characterized by extremely rapid change and development – in the period since this consultation was released developments in AI have, according to some reports, raised the level of threat to previously unprecedented levels.[2]

Measure 6: a power to direct the management of cyber threats

Meridian is supportive of measure 6. In exceptional circumstances, cyber threats to critical infrastructure may pose risks of such scale and severity that as a last resort government direction may be necessary to protect national security. The example of a direction to accept support from the NCSC is a good one. It would be helpful if other examples could be specified in the eventual legislation. The protections listed in the box on page 18 are good ones as are the legal and natural justice protections.

Given that electricity generation and control systems are safety-critical and technically complex, Meridian considers it essential that any direction power is exercised with strong operational engagement, clear reliance on sector-specific expertise, and explicit recognition of health, safety and system-stability considerations.

Meridian also recommends that measure 6 is designed to complement existing governance and accountability frameworks, rather than cut across them. As with measure 5, the board's role should remain one of oversight and assurance, with management responsible for safe execution, and liability settings should be coherent with the fact that directions may need to be implemented under time pressure and with incomplete information. In practice, we would expect that the most effective application of measure 6 would often involve directions to accept government support and coordination, rather than prescriptive instructions on technical operations. The legislation should also anticipate and

[2] See for example this report relating to the development of the Claude Mythos model by Anthropic: https://www.bbc.com/news/articles/c2ev24yx4rmo

provide for appropriate undertakings to be provided by government in situations where a government direction conflicts with an entity's own expert advice from its managed defence partners.

Compliance and enforcement

Meridian supports a proportionate and staged framework for compliance and enforcement. It should prioritise capability uplift, clarity of expectations, and continuous improvement. We consider enforcement will be most effective where primary accountability sits with the entity. Escalation should be in line with the severity and persistence of non-compliance. As cyber security is characterised by evolving threats and judgement-based obligations, enforcement should reinforce good risk-management behaviour and transparency, rather than assume that all cyber incidents are preventable.

With respect to compliance and enforcement in respect of directors, and as indicated above, Meridian agrees with the submission made by the IoD. In particular, we would like to highlight the following recommendations from the IoD submission, which we consider to be especially relevant:

- the primary compliance duty should sit with the critical infrastructure entity
- penalties for core obligations sit primarily with the entity and be set at a level that is proportionate and comparable with peer jurisdictions, with personal criminal liability for directors removed
- the board's role be framed clearly as one of oversight and assurance, with management responsible for implementation
- the regime recognise that directors already hold duties under the Companies Act and equivalent legislation, and avoid duplicating duties that already exist
- minimum cyber risk management requirements be supported by clear guidance, realistic implementation pathways and a credible approach to assurance
- any attestation model sit with the entity and management
- the regime should recognise the reality of third-party and supplier dependence and avoid exposing management of CIEs and directors for failures in environments they do not control
- the regime be implemented through a staged compliance model, supported by practical guidance and a regulator capable of lifting standards across the system
- the implementation model should include a focus on lifting capability across the system, including management capability, board capability and assurance provider

capability, and recognise the importance of independent directors in challenging, influencing and supporting capability uplift

- the regime should make clear that entities and boards are to be judged on how they identify, prioritise and manage material cyber risks over time, rather than on an assumption that every cyber incident can be prevented

Meridian strongly agrees that effective cyber security requires strong board oversight and attention. However, as the regulatory regime will be based on subjective and judgement-based concepts (such as “risks that are material” and “reasonably practicable”), personal criminal liability for directors is unlikely to improve compliance or resilience.

Closing remarks

Given the sensitivity of the subject matter we ask that this submission is treated as confidential and commercially sensitive. We would be happy to discuss this feedback, and we welcome future engagement as this work evolves.

Nāku noa, nā

Jason Woolley / Evealyn Whittington
General Counsel / Senior Regulatory Specialist

Submitted on behalf of Meridian Energy Limited

General questions

Question	Meridian response
Is your entity, based on the draft thresholds set out on pages 10 and 11, likely to be a critical infrastructure entity?	Yes. Meridian is a generator of electricity and would clearly come within the definition.
What one-off capital costs do you expect to incur to comply with each measure, if any (e.g. the cost of developing new reporting systems)? Please provide a range between expected costs and highest possible costs.	As Meridian already has in place a cyber security and risk management programme that is aligned with internationally recognised cyber security frameworks, our expectation is that the additional costs to comply with the proposed measures would be relatively small.
What ongoing capital costs do you expect to incur to comply with each measure, if any (e.g. the cost of additional investments in resilience to meet the requirements of the risk management programme)? Please provide a range between expected costs and highest possible costs.	As indicated above, as Meridian already has in place a cyber security and risk management programme that is aligned with internationally recognised cyber security frameworks and is committed to maintaining, updating and improving that programme, we do not expect to incur any additional ongoing capital costs of significance.
What ongoing operational costs do you expect to incur to comply with each measure, if any (e.g. the cost of undertaking a risk assessment, as required by the risk management programme)?	For the reasons given above we do not expect the additional operational costs to be significant.
What assumptions have underpinned these cost estimates?	See answers above.

Specific questions

	Question	Meridian response
Defining critical infrastructure		
1	Would you support the proposed approach to defining critical infrastructure and critical infrastructure of national significance, and if not, what changes would you recommend?	Yes.
2	Do you consider any essential services have been included or excluded that should not be? If so, what services are they and why should they be added or removed?	No.
3	Do you think the example thresholds for defining critical infrastructure have been set appropriately and provide sufficient clarity as to what level of service provision constitutes critical infrastructure? If not, what alternative thresholds would you support, and why?	Further clarification could be provided. For example, it's not completely clear to us how electricity retailing would be treated.
4	In addition to interdependencies and consequences of a disruption, are there other factors you think should be considered in assessing whether an asset should be declared critical infrastructure of national significance?	We note that the consultation also refers to the severity and extent of harm. Our view is that this is also an important factor in assessing whether an asset should be classed as a CINS.
5	Do you agree that the Minister responsible should have the ability to designate or exempt critical infrastructure entities? If not, what alternative approach would you support, and why?	Yes, we are supportive of this. Allowing the Minister to designate or exempt CIEs, will allow the regulation to adapt over time. We note that the proposal is to couple this with a process around notification and feedback from the affected entity. Our view is that this is also essential.
Improving information sharing and collection on threats and vulnerabilities		
6	Do you agree with the proposed approach to protecting the data shared? If not, what alternative provisions would you suggest and why?	Yes.
7	If you are likely to be deemed a critical infrastructure owner or operator, what effect would having all essential infrastructure providers participating in the formal information exchange, rather than just other critical infrastructure entities, have on your willingness to participate?	The more parties that participate the greater the risk of breach of confidentiality. Meridian would have to assess this further once it has a full list of all entities participating.
8	If the government required regular reporting of all cyber incidents, how frequently do you think this	We suggest every 6 months to start with.

	information should be required (e.g. every quarter, every six months)?	
9	Do you consider the proposed definition of a cyber incident can be given effect within your existing approach to enterprise risk management? If not, what alternative definition would you recommend?	Yes, but it would assist if the definition was made more granular e.g. a materiality threshold applied.
10	Would a requirement to report significant cyber incidents make you less willing to report other cyber incidents voluntarily?	No.
11	Do you consider using the criteria of serious and above for cyber incidents that should be reported within 72 hours are appropriate. If not, what criteria for reporting would you recommend?	Yes.
12	What impact do you think the requirement to report significant cyber incidents could have on your incident response process? For example, would you need to involve lawyers to determine what incidents to report and when?	We don't think there would be any need to involve lawyers provided the definitions are clear enough.
Introducing minimum cyber risk management requirements across the critical infrastructure system		
13	Are any of the specific words proposed to set the requirements of the risk management programme on page 15 likely to conflict with your existing approach to risk management in a way that requires you to make significant changes to these processes, rather than build on what already exists.	No. However, we note organisations typically align with international frameworks, rather than comply with them in a strict legal or regulatory sense.
14	Do you agree that critical components should be defined in a way that aligns with the scope of the requirements in the emergency management system? If not, what alternative scope would you recommend, and why?	Yes.
15	Do you consider that the concept of a risk that is material can be given effect to within your existing approach to enterprise risk management? If not, what alternative approach to defining the level of risk that must be treated would you recommend, and why?	Yes. Again, if more detail can be provided in the definition of the relevant risks that would be helpful.
16	Do you consider that the threshold for treating risks should be set at so far as reasonably practicable? If not, what alternative language to set the scope of risks to be treated would you recommend, and why?	Yes, in general. Some explicit recognition of costs and how those are to be considered within the threshold should also be included.

17	Do you support the risk management programme complying with a cyber security framework that is endorsed by the NCSC or recognised internationally?	As noted in the submission, Meridian recommends that this obligation be framed around aligning with a given framework, rather than compliance as such.
18	Do you agree that government should not prescribe the international internationally recognised cyber security frameworks that are acceptable if compliance with an international cyber security framework were required? If not, what framework(s) would you suggest should be included on such a list, and why?	Yes.
19	Do you consider that a requirement for third-party vendors that have operational control over critical components, to support responsible entities to comply to the extent reasonably practicable, is important to the effective implementation of the risk management programme? Do see any unintended consequences? If so, what do you consider those to be?	Yes, we agree this is important.
20	Do you consider that there are alternative ways for the government to recognise that compliance with other regulation is equivalent to the minimum requirements for cyber risk management? If so, what do you propose?	No.
21	Do you consider there is a more effective way to ensure compliance than to attach responsibility for minimum requirements for cyber risk management to individual directors? If so, what would you propose?	We believe the compliance responsibility should sit at the entity level. See comments in the body of our submission.
22	Do you have a preference on how responsible entities should demonstrate compliance with minimum requirements for cyber risk management?	We support the proposals in the paper.
Ensuring effective management of cyber threats impacting national security		
23	When responding to a cyber incident for national security reasons, what support from government is most helpful to aid the restoration of essential services?	Access to advice from key government agencies, if needed, would be most helpful.
24	Do you think the thresholds for the use of the last-resort power are appropriate? If not, what changes would you propose?	Yes.

25	Do you think that the protections and rights for entities subject to the last-resort power are appropriate? If not, what changes would you propose?	Yes. Government undertakings to protect entities required to comply with directions should also be considered.
Ensuring mandatory requirements improve the cyber security of the critical infrastructure system		
26	Do you consider that the breaches are appropriately mapped to compliance and enforcement tools? If not, what changes would you propose?	Meridian supports a graduated and proportionate approach to compliance and enforcement. However, we consider that some elements of the breaches and associated tools would benefit from further refinement. A number of serious and critical breaches are related to judgement-based governance and risk-management obligations. And the cyber threat environment is extremely fast moving. Meeting the standard necessary to reasonably protect against threats is and increasingly onerous and exacting task. Criminal penalties are most effective when applied to clearly wrongful conduct. The compliance framework would be strengthened by placing primary reliance on entity-level enforcement for cyber risk management obligations, supported by graduated regulatory tools.
27	Do you support the proposed approach to compliance and enforcement where an entity breaches requirements across two or more regulatory regimes? If not, what alternative would you propose?	Yes.
28	Do you agree that penalties in respect of compliance with minimum cyber security requirements should apply to the entity's directors as well as to the organisation as a whole? Why or why not?	No. See the comments in the body of our submission.
29	Do you perceive any perverse outcomes as a result of directors being individually liable for the most serious breaches of the regime?	Yes. See the comments in the body of our submission and in the submission of the IoD.