17 April 2026

Department of Prime Minister and Cabinet

Level 8 Executive Wing
Parliament Buildings
Wellington

By email: criticalinfrastructure@dpmc.govt.nz

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

1. Thank you for the opportunity to make a submission on this Discussion Document.

2. We set out below some background information about Orion, before we address your various questions in the Appendix to this letter. Overall, we broadly support the proposals outlined in the Discussion Document.

Background information

3. Orion is responsible for the electricity distribution network across Central Canterbury, covering both rural and urban areas, including Christchurch. The network spans over 8,000 square kilometres, with over 230,000 connections (or installation control points "ICPs"), making Orion the third largest Electricity Distribution Business (EDB) in New Zealand.

4. Orion is a Lifeline Utility for the purposes of the Civil Defence Emergency Management Act 2002. Orion has a statutory duty under this legislation to ensure it is able to function to the fullest possible extent, even though this may be at a reduced level, during and after an emergency.

5. Orion is a Council-owned company, with its shareholders being the Christchurch City Council (via Christchurch City Holdings Ltd) and the Selwyn District Council. Orion also owns Connetics, an industry service provider, and together they form the Orion Group.

6. Central Canterbury is experiencing rapid growth and change, with Christchurch at its centre. Electricity distribution is fundamental to the wellbeing and economic prosperity of the region. Orion's services are crucial for both residents and businesses, and Orion is playing a key role in New Zealand's transition to a low carbon economy.

Orion New Zealand Ltd
565 Wairakei Road
PO Box 13896
Christchurch 8141
+64 3 363 9898
oriongroup.co.nz

7. In this context, Orion's Group Purpose of "Powering a cleaner and brighter future with our community" is central to all we do. As Aotearoa New Zealand transitions to a low carbon economy, the energy sector has a critical part to play, primarily through electrification. Orion has established its purpose to be a vital player in that transition for our community and our region.

8. Looking ahead, the ongoing advancement of our digital capacity is essential for effective network management and the facilitation of customer choice in emerging technologies. Nevertheless, as technology progresses and digital capabilities expand, the risk of cyber-attacks also increases, with incidents becoming both more frequent and sophisticated. Robust cybersecurity is non-negotiable. We are consistently enhancing our cyber defences and monitoring capabilities to maintain network reliability, protect infrastructure, and ensure the security of customer data.

9. With that background in mind we set out our answers below to the various questions raised. We also note that we are a member of Electricity Networks Aotearoa (ENA) and we support the ENA's submission on this Discussion Document.

10. If you have any questions about this submission, please feel free to contact Vivienne Wilson, Policy Lead at vivienne.wilson@oriongroup.co.nz . [redacted]

Yours sincerely

Vivienne Wilson
Policy Lead

Orion

APPENDIX

General Questions

Question	Response
Is your entity, based on the draft thresholds set out on pages 19-23, likely to be a critical infrastructure entity?	Yes. Orion is likely to be a critical infrastructure entity. We provide electricity distribution services as defined in section 54C of the Electricity Industry Act 2010 and we have over 230,000 ICPs.
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.	[redacted]
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.	We are unsure at this stage.

Orion New Zealand Ltd
565 Wairakei Road
PO Box 13896
Christchurch 8141
+64 3 363 9898
oriongroup.co.nz

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)? Please provide a range between expected costs and highest possible costs.	We anticipate that Opex will largely consist of the reporting costs. The costs will depend on the level of compliance imposed and will also be affected by the requirements of our integrated leadership team (ILT) and the requirements of the Orion Board.
What assumptions have underpinned these cost estimates?	Noting our comment above, we are also hoping that there will be scope for harmonisation between the requirements under this proposal and other existing legislative requirements. We are keen to avoid duplication, and reducing the administrative burden will be key. We note that page 17 of the Discussion Document refers to "*Many critical infrastructure entities already manage cyber risks, whether to address the recommendations of the NCSC, to meet sector-based guidelines or requirements, to satisfy prudent governance, or for commercial reasons.*" It also notes that "*Wherever an entity is meeting the requirements through adherence to sector-based regulations, the relevant sector regulator would remain responsible for monitoring compliance. If requirements were not met, this would breach the requirements of both regimes. Details on how this would be managed in a way that avoids double jeopardy is provided on page 19.* *For entities subject to price-quality regulation by the Commerce Commission, any investments required to comply with minimum requirements could be able to be offset with additional revenue*." EDBs are regulated under the Commerce Act 1986, so that all EDBs are subject to information disclosure regulation (s54F); and 16 of 29 EDBs are subject to default/customised price-quality regulation (s54G), by virtue of not meeting the definition of consumer-owned (s54D).

	Orion is required to comply with information disclosure regulation, as well as default price-quality regulation.[1] It would be helpful if we are able to draw on one regime to assist compliance with another regime. Another potential area of crossover will be compliance with the Privacy Act 2020 and notifiable privacy breaches. However, whatever the final form of the obligations imposed on critical infrastructure entities, it is important that EDBs have a corresponding uplift in revenue to meet these costs. Treating this expenditure as "business as usual" is likely to be unsustainable in the long-term and we ask that funding provision is taken into account when designing this new regime. We understand that you have had discussions with the Commerce Commission about the connectedness of the two regimes.

[1] We are in the process of applying for a customised price path.

Defining Critical Infrastructure

Question	Response
Would you support the proposed approach to defining critical infrastructure and critical infrastructure of national significance, and if not, what changes would you recommend?	As we understand the Discussion Document, various "components" will be designated as critical infrastructure. Components could include assets, information, networks, systems, suppliers, people and processes. The draft thresholds set out in the Discussion Document clarify the type and level of service provision that meets the definition of critical infrastructure. However, the Minister will be able to designate certain components or entities as critical infrastructure, or exempt entities as the case may. Therefore, obligations may attach to entities or components. Presumably an entity that is responsible for critical infrastructure may also be responsible for essential infrastructure at the same time. Obligations might attach to one part of their business and not other parts. We think this will need to be more clearly expressed in any legislation as it must be clear who is responsible for compliance with the regime and in relation to what components. Subject to our comments above, we support the proposed approach to defining critical infrastructure and critical infrastructure of national significance.
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?	We think further consideration should be given to electric vehicle charging station operators. As the electric vehicle fleet grows, these operators could assume growing significance in New Zealand. The same can be said for energy aggregators[2] that combine distributed energy resources into controllable portfolios.

[2] Energy aggregators are distributed energy resources (DERs) that are pooled together into a single controllable portfolio. They act as intermediaries between small scale assets and electricity markets or grid operators. Energy aggregators rely on digital software platforms and real time data to maximize efficiency and performance, unlock flexibility as well as allow market participation which individually managed assets can't access alone. See https://www.gridx.ai/knowledge/energy-aggregators-in-flexibility-markets

Question	Response
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?	We support the current proposed approach but we query whether the single measure for EDBs should be the number of ICPs. Some networks cover a large area of New Zealand but with a smaller number of ICPs. Some networks are managed together, and it may be appropriate to consider those networks together. (Costs could therefore be shared which would ease the regulatory burden on smaller communities/networks.) Smaller EDBs will supply electricity to other essential services that if interrupted will cause considerable disruption.
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 want to be involved in further discussions about the inclusion of suppliers as components of critical infrastructure. As mentioned above, Orion owns Connetics, an industry service provider. Depending on the obligations imposed on entities and their suppliers, there may need to be changes to contractual arrangements which could be time consuming and costly to implement. Is it also envisaged that suppliers will be New Zealand entities or will this also include overseas suppliers? Again, aside from negotiating changes to existing contracts, it is not clear to us how we could impose additional obligations on overseas suppliers unless current contractual arrangements allow for regulatory change.
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 agree with this approach but we would also expect there to be some engagement with entities before their status changes or there is a change in status of other critical components for which the entity is responsible.

Improving information sharing and collection on threats and vulnerabilities

Question	Response
Do you agree with the proposed approach to protecting the data shared? If not, what alternative provisions would you suggest and why?	We note that currently there is a voluntary information sharing process within the electricity distribution sector that works well. But, in our view, there does need to be considerable work/analysis completed before additional cross sector information sharing can take place. See below and our comments on the next question. For example, on page 13 of the Discussion Document, it notes that information shared or collected would be held in strict confidence. There are three bullet points which subsequently describe how the government could use and share the information. Any breach of these protections by a government agency would be an offence. We agree with the protections noted but we would also like to see more details of how the gathering and use of information would work in New Zealand. What protections will be in place for the entities that are sharing the information? How will the regime work in light of other contractual provisions that may prevent disclosure?
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?	In our view, there will need to be limits on the information shared across sectors. As we understood the initial proposal, the original aim was to allow smaller companies to leverage the learnings of larger companies (that have greater resources). We think that some information shared within the sector may not be appropriate to share outside of the sector. Furthermore, there would need to be adequate security controls and protections around the information exchanged. We also think there needs to be an exclusion from the application of the Official Information Act 1982 where information is provided to government entities covered by that Act.

Question	Response
If the government required regular reporting of all cyber incidents, how frequently do you think this information should be required (e.g. every quarter, every six months)?	We suggest yearly reporting for all cyber incidents. (This assumes that the proposed requirement to report incidents within a 24-hour and 72-hour window does not cover all incidents.)
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?	The proposed definition reflects the definition in Australia.
Would a requirement to report significant cyber incidents make you less willing to report other cyber incidents voluntarily?	Even if there is a requirement to report significant cyber incidents, Orion would still share other cyber incidents within the electricity distribution sector.
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?	Further discussion about timeframes, the form of warning and reporting is needed. It can take between 24-72 hours to determine whether an entity is under attack. In our view, a full report not later than 72 hours will not be practicable as it is most likely there will still be an ongoing investigation, and the primary focus is on responding to the incident. We are conscious that it is not helpful to report "false positives". We note that in Australia, early reporting by telephone is accepted. We also note that under the EU system, the following applies, "*Three-stage process: 24 hours for early warning, 72 hours for initial notification, 1 month for final report. Only significant incidents (those disrupting services) need reporting.*"[3] One month for a final report may be a more realistic timeframe.

[3] See https://www.homeaffairs.gov.au/cyber-security-subsite/files/independent-review-soci-act-final-report.pdf

Question	Response
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?	As a lifeline utility, Orion has adopted the CIMS (Critical Incident Management System) framework for our incident response process. Our CIMS protocols include Orion's response to a cyber event. As noted above, the focus must remain on responding to the incident/attack. But reporting requirements should also align with existing incident response and escalation processes and avoid creating parallel regimes. If there is a way to combine notification procedures that would be helpful, such as where an attack also results in a notifiable privacy breach under the Privacy Act 2020. Importantly, insurance terms and conditions should also be considered and protected. We would not want to invalidate coverage under our insurance policies by reason of a notification, or by any other requirements specified by legislation. Page 14 of the Discussion Document discusses how reporting on cyber incidents could be used. The Document notes that "*the government's priority upon receiving an incident report is swift remediation and recovery, rather than immediate compliance action. The information would not be used for regulatory purposes*." It is not clear to us what is meant by saying that it will not be used for regulatory purposes when the Document goes on to say that "*this limited use obligation would not provide a safe harbour from legal liability or prevent a regulator from acquiring the same information directly from the entity*." Our preference is that safe harbour protections are necessary to ensure good faith reporting is not used punitively by regulators or in litigation.

Introducing minimum cyber risk management requirements across the critical infrastructure system

Question	Response
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?	Generally speaking, effective risk management is fundamental to achieving our strategic focus areas: maintaining a safe, reliable, and resilient network; enabling a highly utilised and accessible network; and supporting the wellbeing and prosperity of our community. Page 15 of the Discussion Document broadly sets out an approach that is compatible with Orion's approach, and the risk management approach referred to in the Electricity Distribution Information Disclosure Determination 2012.[4] However, we do not agree with **requiring** a cyber security framework that is endorsed by the NCSC or recognised internationally, such as the US National Institute of Standards and Technology Cybersecurity Framework (NIST CSF) or ISO/IEC 27001:2022. We think **alignment** would be a satisfactory standard – see our comments below. By way of information, risk management at Orion aligns to ISO 31000. Additionally, Orion is positioning its asset management to ISO 55000. We are also currently aligning with the Australian Energy Sector Cyber Security Framework (AESCSF).

[4] For example, see Attachment A and the requirements of asset management plans, clause 14. *"Asset risk management forms a component of an **EDB's** overall risk management plan or policy, focusing on the risks to assets and maintaining service levels. **AMPs** should demonstrate how the **EDB** identifies and assesses asset related risks and describe the main risks within the **network**. The focus should be on credible low-probability, high-impact risks. Risk evaluation may highlight the need for specific development projects or maintenance programmes. Where this is the case, the resulting projects or actions should be discussed, linking back to the development plan or maintenance programme."*

Question	Response
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 we agree with this approach. As a lifeline utility, Orion's approach to emergency management aligns with NEMA civil defence requirements and principles. Our focus is on the 4 Rs, in other words reduction, readiness, response and recovery. Orion's approach to Emergency Management is also enterprise wide. We take the same approach to risk reduction and readiness for cyber events as we do for civil defence emergencies such as weather events and earthquakes.
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?	Our existing approach includes the following: • We identify risks that could affect our ability to deliver on our purpose or objectives. • We review our risks regularly and update our risk profiles accordingly. • We assess the likelihood and impact of each risk and prioritise them based on their potential impact. • We manage risks by implementing appropriate controls, procedures, and policies. • We ensure that these controls are regularly reviewed and updated. We do not necessarily agree with the starting point of a risk that is material.
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?	See our comments above.

Question	Response
Do you support the risk management programme complying with a cyber security framework that is endorsed by the NCSC or recognised internationally?	In accordance with our comments above, we do not support mandating a particular cyber security framework. Within these frameworks we also note that there are different maturity indicator levels. For example, within the AESCSF, there are 3 Maturity Indicator Levels (MIL). Would the Government also want to specify which MIL an entity must meet and by when? We think these decisions are best left to entities themselves.
Do you agree that government should not prescribe the 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?	As above, Orion does not agree with mandating formal certification. Alignment with a recognised framework should be sufficient to lift cyber security outcomes without creating an unnecessary compliance burden.
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?	We are aware that the energy sector faces unique challenges in safeguarding cybersecurity across operational technologies, SCADA systems, and legacy infrastructure. Vendor support for aging assets may be limited, and the increasing complexity, along with evolving expectations and uses of operational technologies, adds layers of challenge to risk management. These factors may necessitate customised strategies that extend beyond conventional IT practices. Therefore, the ability for EDBs to choose the right framework(s) is critical to provide flexibility to align with maturity and controls standards.

Question	Response
	With the above comments in mind, requirements for third-party vendors that have operational control over critical components to support responsible entities to comply to the extent reasonably practicable will be welcome. But the extent to which they may be able to support may be limited.
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?	We refer to our comments on page 4 of this submission where we noted that we are also required to comply with the requirements of the Commerce Act 1986, including information disclosure requirements and price quality regulation. The information disclosure requirements could form a basis for compliance with the requirements of this new regime. Reducing duplication of regimes will lower costs for EDBs, and therefore costs for our customers.
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 acknowledge there are benefits to requiring individual directors to certify that particular requirements have been met. It leads to greater awareness and involvement at board level in the matters requiring certification. This can strengthen risk awareness and accountability. However, given the nature of these sorts of obligations, we think it is important to build-in adequate defences, such as a reasonable steps defence and for the government to provide clear guidance on expectations. Otherwise, the nature of the obligations could encourage behaviour that is framed solely around protection liability, and encourage overly risk averse decision-making. We say more about this approach in relation to the possible imposition of criminal penalties.
Do you have a preference on how responsible entities should demonstrate compliance with minimum requirements for cyber risk management?	There has been some discussion at the recent consultation meetings about the mandating of independent audits. Orion does not agree with an independent audit requirement. There is limited auditor capacity in the New Zealand market. We consider that self reporting via a selected framework on a yearly basis should be sufficient.

Ensuring effective management of cyber threats impacting national security

Question	Response
When responding to a cyber incident for national security reasons, what support from government is most helpful to aid the restoration of essential services?	We appreciate the support of the National Cyber Security Centre and its various services (See Welcome to the National Cyber Security Centre). We all have partners so any information that may assist is useful. We appreciate a governance role and the provision of relevant information that we may not have from a clearance perspective. We are of the view that these services should be free.
Do you think the thresholds for the use of the last-resort power are appropriate? If not, what changes would you propose?	We note that in the legislation passed by the Canadian Parliament,[5] the Governor in Council has a similar power to issue directions and before doing so must consider (a) its operational impacts on affected designated operators; (b) its impact on public safety of Canadians; (b.1) its impact on the privacy of Canadians; (c) its financial impacts on affected designated operators; (d) its impact on the delivery of vital services and vital systems to consumers; and (e) any other factor that the Governor in Council considers to be relevant. Similar considerations may also be relevant in New Zealand where the Minister has a power to direct the management of cyber threats for national security reasons.

[5] See the Critical Cyber Systems Protection Act 2026 at https://www.parl.ca/documentviewer/en/45-1/bill/C-8/third-reading

Question	Response
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?	We weren't sure what is meant be "limits on the acquisition of property" – would this be a provision similar to section 35 of the Australian *Security of Critical Infrastructure Act 2018?* An indemnity against legal liability when the entity is subject to a Ministerial direction will be very important. The ability to appeal to the Minister will need to be clearly spelt out. Presumably a right to statutory review will follow the usual process under the Judicial Review Procedure Act 2016. Specific provisions about the use and disclosure of information may also be required.

Ensuring mandatory requirements improve the cyber security of the critical infrastructure system

Question	Response
Do you consider that the breaches are appropriately mapped to compliance and enforcement tools? If not, what changes would you propose?	Yes, we largely agree with the table set out on page 20 of the Discussion Document.
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?	We agree that a responsible party should not be punished twice for breaching more than one regulatory regime. In the context of the electricity distribution sector, it would need to be carefully thought through as to which regulator is best placed to be responsible for the regime.

Question	Response
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?	Under the Companies Act 1993, directors are obligated to exercise their powers with care, diligence, and skill (s137). They must act in good faith and in the best interests of the company (s131), ensuring that their actions align with the company's objectives. Further, directors must exercise their powers for a proper purpose (s133), avoiding irrational decision-making. Recent legal cases concerning director liability indicate that this topic remains dynamic and evolving. In addition, New Zealand already imposes significant accountability on directors through civil liability, public enforcement, pecuniary penalties, compensation orders, and director disqualification. Consequently, we question whether the imposition of further criminal penalties on directors would be an appropriate or necessary punishment. That said, if director criminal liability is pursued, we suggest that the Government issues guidance on director cybersecurity duties as well as provide director cybersecurity governance education programmes. There would also need to be a transitional implementation period.
Do you perceive any perverse outcomes as a result of directors being individually liable for the most serious breaches of the regime?	As noted by Electricity Networks Aotearoa in their submission, concern about the scale of penalties could deter suitably qualified people from taking on governance roles and may encourage overly risk-averse decision-making. Further, monetary penalties imposed on an EDB reduces funding that would otherwise be invested in regulated infrastructure as set out in Asset Management Plans. Ultimately, these costs are borne by consumers through higher prices or deferred investment, without necessarily improving cyber resilience outcomes.