17 April 2026

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

Submission to:

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

Preliminary matters

Our submission does not contain confidential information.

Transpower's address for service is:

Transpower New Zealand Limited
PO Box 1021
Wellington 6140

Attention: Jo Mooar, Senior Corporate Counsel
Email: joanne.mooar@transpower.co.nz
Phone: 04 590 6060

Introduction

As the owner and operator of critical infrastructure, Transpower New Zealand Limited welcomes the opportunity to comment on *Enhancing the cyber security of New Zealand's critical infrastructure system* (**Discussion Document**).

The Discussion Document explicitly captures our infrastructure in 3 respects:

- Operation of the National Grid;
- Operation of the wholesale electricity market; and
- The Cook Strait telecommunications cables.

Summary of position on the Discussion Document

We welcome the Discussion Document and support the proposed direction to lift the cyber security of critical infrastructure through outcome and risk-based approaches and stronger information sharing. We agree with the Prime Minister's introductory comments that any new regime must be "practical, flexible and responsive."

However, the administrative burden, and costs, of regulatory change could be significant. In order for the benefits to outweigh the costs, any reform must be tightly scoped, contain appropriate protections, be staged for practical uplift, and paired with government uplift on intelligence, supply chain assurance, support in attaining personnel clearances for staff of infrastructure of national significance (**CINS**) organisations and major incident co-ordination.

The Discussion Document proposes a tiered approach to defining infrastructure by the level of criticality of some of its components. While we support a tiered approach, it needs to be handled with discipline. The Discussion Document envisages a subset of critical infrastructure being treated as CINS, with an early focus on interdependencies and potentially stronger obligations over time. It is important that criteria for determining CINS are transparent, consulted on, and stable, so designations do not shift unpredictably and undermine long-term planning.

We support adherence to existing recognised risk management frameworks. While the Discussion Document advances a risk-based approach, some prescriptive (and additional) requirements appear to be proposed for CINS. We oppose these prescriptive requirements, given the learnings from the Security of Critical Infrastructure Act 2018 (**SOCI Act**), and the challenges from the regime having prescriptive maturity-based targets. Transpower supports stronger information sharing, with a preference to building any formal exchange from existing trusted sector arrangements, rather than creating a parallel forum. The approach to cyber-security uplift for critical infrastructure described in the Discussion Document is best met by focusing on outcomes: secure handling with clear purpose limits, actionable intelligence, supply chain assurance (elements within existing TICSA arrangements) and rapid coordination when interdependencies create system-wide risk.

As drafted, the Discussion Document leans heavily on infrastructure providing government with information, but there is no information flow in return. A robust, efficient, regime must have a timely two-way information flow. This information flow matters in a threat environment shaped by geopolitical tension, where state-sponsored and other well-resourced groups pursue long-term access and strategic advantage, not quick disruption alone. Government holds unique visibility and international partnerships, including Five Eyes channels. The regime should support critical infrastructure with rapid, actionable threat advice, indicators, and coordination back to operators from government.

The Discussion Document proposes some protections for information sharing. These protections need to be clearly defined, and available from the outset. There is a need for safe harbour and strong legal settings, so reporting does not default to being slow, defensive and legally reviewed, both during and after events. A clear "limited use" and non-punitive approach is a prerequisite for timely, candid reporting. This approach is also needed to protect existing voluntary engagement with the National Cyber Security Centre (**NCSC**).

Transpower understands the need for compliance with any new regime to be demonstrated. We suggest attestation by management is appropriate. We oppose a regime with penalties and offences being developed from the outset. There is no evidence to suggest a punitive regime, including one involving director liability, is warranted. Further, perverse outcomes could result if staff are diverted from cyber security tasks to contributing to any defence.

We also oppose the imposition of an additional regulator and/or additional or duplicate regulation being applied by existing regulators. Transpower is already subject to regulation by the Commerce Commission and the Electricity Authority, both capture resilience to a certain extent (primarily through reliability requirements and service quality measures).

It is important to note that Transpower's submission is limited to cyber security. We have not provided our responses in a way that could be "lifted and shifted" into broader reform on infrastructure resilience more generally. Infrastructure is complex –other threats require specific responses that are different from enhancing cyber security.

Learnings from SOCI

Our understanding from our Australian peers after the implementation of the Commonwealth Government's SOCI Act is that the framework set up a complex burden of compliance plans and audits. Compliance thresholds, while designed to encourage vigilance were based on "industry best practice[1]," a target that continued to move while not matched by investment horizons for critical systems. Costs were also increased through the need for onshoring of data and technical support limiting cost efficiencies gained from cloud-based computing. The standards also created blanket requirements and did not consider the risk-value trade-off between infrastructure used to serve rural areas versus major capital cities. This framework has been expensive to comply with and has led to a significant ongoing regulatory burden with a range of unintended consequences. The additional costs will ultimately be paid for by consumers. Care should be taken to not repeat the mistakes of the Australian regime.

Alignment between cyber security regime and existing regulatory settings

Many of the entities that will be considered critical infrastructure under the new regime are already regulated. We consider that the new regime needs to be developed in a manner that is cognisant of those existing regulations and regulators. Transpower has two regulators – the Commerce Commission and the Electricity Authority.

One of the Electricity Authority's functions is to promote "reliable supply by, and efficient operation of, the electricity industry for the long-term benefit of consumers." To an extent, this function captures resilience of the electricity system (although, not inter-related infrastructure operators or related entities).

Unless there is alignment between the requirements of the proposed regime and the Commerce Commission's role in determining prudent and efficient expenditure, Transpower may not have sufficient funding to undertake all the actions required under the new regime, or would need to

[1] By contrast, Transpower's key regulator expects us to meet "Good Electricity Industry Practice (Electricity Industry Participation Code).

consider reducing expenditure on meeting other transmission services[2]. As a result, we consider that the imposition of any obligations under the proposed regime needs to be considered against funding constraints and the regulatory regimes that all critical infrastructure entities operate in.

Specific questions

We address the questions in the Discussion Document of most relevance to Transpower below. Some of our answers are brief. We are happy to discuss any of our answers and the Discussion Document with you.

Note that we have not answered the questions in relation to costs posed on page 22 of the Discussion Document. The options, and combination of options, are not articulated in a manner that enables them to be costed at this stage. However, we expect costs in relation to overheads will increase due to any reform.

Defining Critical Infrastructure

Would you support the proposed approach to defining critical infrastructure and critical infrastructure of national significance, and if not, what changes would you recommend?

The Discussion Document proposes identifying certain components of infrastructure as critical, with some components identified as being of national significance.

We consider that clarity is crucial. Critical components need to capture certain operational technology, information technology, data, suppliers, people, and processes tied to service delivery. The proposed definition of "*components*" (page 9) is suitably broad.

We support a principles-based approach, with thresholds. We support the detail being contained in regulation, rather than primary legislation, so that thresholds can remain flexible over time.

We also support the identification of *some components* as being of national significance. This identification should be evidence based and security sensitive, with transparent criteria and a mandatory requirement for engagement and input from the infrastructure entity.

While we are comfortable with the approach taken in the Discussion Document, we are concerned that the terms "*critical infrastructure*" and "*critical infrastructure of national significance*" are much broader than components, and more aligned with the criticality of a network[3]. We consider that it would be more appropriate to define "*critical infrastructure components*" and "*critical infrastructure components of national significance.*"

Do you consider that any essential services have been included or excluded that should not be? If so, what services are they and why should they be included.

At a broad level the essential services listed seem appropriate. However, the services are very high level, opening up the potential for services to be missed.

---

[2] A more detailed discussion of Transpower's regulators, and the need for legislative alignment is set out in Transpower's submission on the Emergency Management Bill (No. 2)

[3] It is not uncommon for entire networks to be considered critical or significant in legislation, and secondary documents under legislation. Examples including the Civil Defence Emergency Management Act 2002 and the Resource Management Act 1991.

Do you think the example threshold 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?

The example thresholds in the Discussion Document for the electricity sector are a reasonable staring position – they align with the threshold for being a "generating station" in Part 8 of the Electricity Industry Participation Code.

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?

Transpower supports the Minister being able to designate entities as critical infrastructure/components of critical infrastructure, as this designation needs to be flexible and change over time as systems and interdependencies change. We consider that this Ministerial designation is preferable to any legislation or regulation prescribing what components or entities are captured.

As discussed above, we consider that there should be transparent criteria, and decisions should be made in consultation with potentially affected entities. There should be a mandatory obligation to obtain their views and for them to be considered.

Transpower is less supportive of the proposed exemption capability, given the importance, and integrated nature, of different industries (such as electricity and telecommunications). We are concerned that the exemption capability could impact on our ability to meet any obligations on us, including in relation to the security of electricity supply for New Zealand.

The proposed exemption would be from categorisation as critical infrastructure/components of critical infrastructure. It would mean that the relevant entity would not be subject to the regime at all. The need for exemptions could cut across the regime (unless another regime contained equivalent controls).

Importantly, the need to exempt entities entirely suggests that the costs of any new regime would outweigh the benefits of improved cyber security. Our 2023 submission on Strengthening the Resilience of Aotearoa New Zealand's critical infrastructure system noted issues with the SOCI Act and suggested incremental reform, focussed on lifting capability among entities.

If the new regime is to include exemptions, we consider they should apply to specific obligations, rather than removing an entity from the regime entirely. By way of example, exemptions could apply to compliance, but obligations in relation to information sharing and some form of more limited incident reporting could remain.

Improving information sharing and collection on threats and vulnerabilities

Do you agreed with the proposed approach to protecting the data shared? If not, what alternative provisions would you suggest and why?

Transpower broadly agrees with the proposed approach to protecting shared data. There must be strong confidentiality provisions and strict purpose limitations. Offences for misuse of shared data is essential. We consider that protections should cover competition law safe harbour for good-faith

sharing, secure storage and access controls, and a limited-use model for incident reports to encourage timely reporting.

A classification framework and de-identification, where practical, would also be useful. We consider that industry confidence will rise if protections are enforceable and consistently applied. The objective of this approach should be to speed up official channels for information sharing as much as possible through safe harbour.

If you are likely to be deemed a critical infrastructure owner or operator, what effect would having all essential infrastructure providers participating in a formal information exchange, rather than just other critical infrastructure entities, have on your willingness to participate?

We expect that some components of our infrastructure would reach the critical infrastructure thresholds proposed. We consider that broader participation by all essential infrastructure providers would increase exchange value, given dependencies will often sit below the "critical infrastructure" thresholds.

We consider that willingness by entities to participate would increase if protections and governance are strong and participation expectations are proportionate. A tiered model could be used to balance openness and sensitivity alongside improving relevance.

If the government required regular reporting of all cyber incidents, how frequently do you think this information should be required (eg. every quarter, every six months)?

It is difficult to comment on whether reporting of "all incidents," and the required timeframe is reasonable, in the absence of understanding the benefit that will be gained from the reporting. In particular, how would this reporting feed into information sharing forums and/or sharing from government about threat intelligence, or incident response. In the absence of understanding how the information is to be used to protect, and respond, at a national level, it could be administratively burdensome, and costly.

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?

We note that the definition of a "significant cyber incident" is proposed to be derived from the definition of "serious impact" from the New Zealand Information Security Manual (**NZISM**) – and include an incident that has had, or is likely to have, serious impact on confidentiality, integrity or availability of information or delivery of essential services. The definition of "cyber incident" is to be defined in the same manner, but without reference to an incident's materiality. We have some reservations about this approach to defining cyber incidents. The NZISM definition includes non-critical systems impact, combined with potential for availability of information. While the definition may be broadly workable for operational (OT) systems and able to integrate with Transpower's enterprise risk management, it has implications for the threshold of incident reporting – the bar is too low (as we discuss below).

We consider that a more appropriate definition would involve an actual impact for non-critical services/components and potential (and actual) impacts for critical services/components focussed on

essential services. Further, there should be the ability to reassess the categorisation of an impact as facts emerge during any response.

We also consider that practical implementation of any new regime will improve if non-statutory guidance is developed that clarifies how infrastructure entities are to categorise an impact. In this regard, the discussion document proposes to leave this determination of "serious impact" to the infrastructure entity. Any guidance should include examples that cover confidentiality, integrity, availability, and essential service delivery, including OT contexts.

Would a requirement to report significant cyber incidents make you less willing to report other cyber incidents voluntarily?

Provided protections for sharing of information is credible (as discussed above), we would not be less willing to report less significant cyber incidents voluntarily. However, if reporting is perceived as a compliance trap, we would expect that voluntary reporting by entities would lessen. As discussed later in this submission, how the incremental roll-out of the new regime is achieved will be important to not undermine the benefits that can be gained.

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?

Transpower has reservations about mandating timeframes for event driven reporting. We consider that a "best endeavours" approach would be preferable, with a notification threshold, followed by ongoing communication as agreed (and incident specific). In this regard, we do not consider that high levels of prescription would be helpful. They are likely to detract from restoration.

As discussed earlier, we have reservations about drawing on the NZISM to define cyber incidents. The bar is set too low. We also note that any notification threshold will require flexibility where detection is uncertain, as is the case in OT environments where visibility can lag. We also consider that an impact-based trigger should be used, that is tied to service delivery and safety consequences, rather than a purely technical trigger.

Again, non-statutory guidance could be used to reduce inconsistent interpretation about how to classify an incident (eg. is it an information exfiltration incident vs a critical service availability incident) or apply any notification threshold.

We note for completeness, that we were concerned about a requirement for a "full report" – any expectations about what that entails would need to be clear from the outset.

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?

It is crucial that reporting does not force operational teams to choose between restoration and compliance. Any requirement to report significant cyber incidents will add decision pressure during a response for borderline incidents. Without clear thresholds and safe harbour, legal review may become routine and slow any response.

We note that the Discussion Document refers to safe harbour, including by reference to the Australian regime that only applies to voluntary reporting of incidents. We note that the safe harbour

proposed appears to be limited and not fit for purpose. We would expect to see something more fulsome.

We consider that an efficient regime could involve a pre-defined decision matrix, pre-authorised reporting roles, and the ability to submit an initial report, with caveats, and the ability to refine information subsequently.

It is crucial that any reporting regime is subject to "limited use" and provided on a non-punitive basis – to keep reporting timely and candid and to preserve voluntary sharing with NCSC. We consider that any compliance implications will be counter-productive and impact open communication.

Introducing minimum cyber risk management requirements across the critical infrastructure system

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?

Transpower is comfortable with references to "reasonable person" and "so far as reasonably practicable." These phrases have been subject to interpretation by the Courts and their intent is known. Transpower considers that reference to "reasonably practicable" is appropriate, as cost considerations are relevant. It is important that cost, and the ability to fund, is relevant to cyber security measures (as we discuss earlier in this submission).

Another pressure point is the requirement for third parties with operational control to support compliance, which will drive contract change and adjust responsibilities. With clear guidance and mapping allowances, risk programmes can build on existing processes rather than replace them.

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?

Transpower is comfortable that the list of "infrastructure components" in the Emergency Management Bill (No.2) is equally applicable to cyber security. However, it is important to note that the actual components captured by each regime (even for a single entity) may be different – alignment cannot be a driver in and of itself.

We would expect cyber-relevant components to include OT/IT systems, networks, data, suppliers, people, and processes necessary to deliver the essential service. All these components would be captured by the definition in the Emergency Management Bill (No. 2).

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. Transpower considers that "material risk" can be operationalised using existing enterprise risk management methods, threat scenarios, consequence modelling, and control effectiveness assessment.

The regime should allow proportionality - by size and complexity - while still preventing material risks from being accepted away without justification.

Transpower's understanding is that more guidance and direction is needed by some entities. There needs to be non-statutory guidance to show what a good basic risk assessment and management looks like. It is not common across all organisations.

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?

As discussed earlier, we consider it is important that cost and funding is relevant to the whether a risk can be treated. We support the "so far as reasonably practicable" threshold for treating risks for this reason.

Do you support the risk management programme complying with a cyber security framework that is endorsed by NCSC or recognised internationally?

Transpower supports the risk management programme being anchored in recognised cyber security frameworks (NCSC endorsed or internationally recognised). Alignment on frameworks to be applied will create consistency, as well as a common language for governance.

However, we consider that there is a need for flexibility. There should be the ability to follow defensible equivalents of a recognised international framework. We also note that this flexibility will avoid unnecessary rework, should entities be applying a recognised international framework that does not make its way onto any explicit list. Any rework could be for limited, to no gain, in terms of cyber security.

We do not support the Minister being able to prescribe additional requirements on CINS – in particular, additional measures that entities may need to undertake as part of their risk management programme, and to require entities to take prescribed actions to manage a particular risk or set of risks.

We are also concerned about the uncertainty and potential costs that could follow from any regime that enables additional regulatory requirements to be prescribed by a Minister at any time - the goal posts could keep shifting from a compliance perspective.

We do consider that CINS should be tied to a higher level of compliance with a framework. However, this obligation should be risk and outcome based, rather than based on control maturity only. Any CINS also needs to be appropriately funded through their regulator/s.

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 is required? If not, what framework(s) would you suggest should be included on such a list and why?

Transpower agrees government should not prescribe a closed list of acceptable frameworks. We already anchor our programme, as many other infrastructure organisations do, in recognised cyber security frameworks. A closed list would create avoidable rework, and cost, when an organisation is using a credible international framework that is not named, with little to no security benefit. An

outcome-based test that allows defensible equivalence and mapping is more durable as frameworks evolve.

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 you see any unintended consequences? If so, what do you consider those to be?

We assume that the reference to "operational control" means direct control of critical infrastructure services, such as outsourcing of operations and maintenance. We consider it important that third-party vendors that have operational control over a critical component must support responsible entities in complying. If vendors with operational control are out of scope, risk can remain unmanaged.

However, consequences from this requirement include contract renegotiation cost, supplier churn, the inability of smaller suppliers to meet requirements, and potentially liability disputes during incidents. It would also be important that any regime did not result in duplication of obligations, should the third-party vendor be subject to the regime in their own right.

Shared supply-chain assurance mechanisms across critical infrastructure would strengthen leverage over high-impact third-party vendors, reduce duplicated assurance effort and cost, and improve sector visibility of material supply chain risk. The new regime should provide for a regulator-facilitated approach that defines common assurance artefacts and evidence expectations, with controlled sharing arrangements for vendor assurance outcomes, so entities can rely on a single assessment where appropriate, rather than repeating bespoke reviews.

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?

The Discussion Document proposes the ability for a cyber security regulator to issue a determination that existing regulation is equivalent to the new regime and/or for the other regulator to ensure compliance with the cyber security regime. If made, a determination in favour of the Commerce Commission could potentially ensure alignment between both regimes – by ensuring that Transpower's cyber-security plan and funding of it (for our 5 year regulatory control period), were approved by the one regulator. Without alignment between the two regimes we risk being unable to fund (and therefore implement) our cyber-security plan. A similar determination could possibly be made in favour of the Electricity Authority for our system operator role.

The proposal to issue determinations would provide some efficiency. However, it does not address the substantive duplication of two regimes. Where the cyber security regime and an existing regulatory regime overlap, we consider that the relevant entity could be exempted from the relevant obligation in the cyber security regime. We suggest that the exemption should be to the cyber security regime obligation, as it is likely to be narrower than existing obligations in broader regulation.

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 consider that any reform should proceed in an incremental manner. We do not support a regime with penalties and offences being developed from the outset; there is no evidence to suggest that a punitive regime focussed on individual directors is warranted. Further, existing duties for directors under the Companies Act 1993 already require directors to exercise care, diligence, and skill and to act in the best interests of the company, which includes cybersecurity matters.

Enforcement is by its very nature "after the fact". We would be concerned if any new enforcement regime measured performance of infrastructure components post an event. It is proposed to apply a reasonable person test, and risk mitigation measures so far as reasonably practicable. But, it will always be possible to land on a different option – to do more, to spend more. There will also be surprises. As a result, we query whether a just enforcement regime could be developed.

Do you have a preference on how responsible entities should demonstrate compliance with minimum requirements for cyber risk management?

We consider a staged approach to demonstrating compliance with a cyber risk framework is appropriate. We consider that initial management attestation should be sufficient, and over time it could increase to periodic structured reporting that is aligned to risk and criticality. We consider that assurance for CINS should be engaged by us, and only be required if other mechanisms for demonstrating compliance are not considered sufficient.

We consider that evidence should focus on control effectiveness and risk treatment, not maturity scoring alone. It is important that any reporting is aligned to existing sector requirements, to reduce duplication.

In practice, the core test should be whether the entity can show it understands its material cyber risks to essential service delivery, has prioritised treatment decisions against those risks, and is executing a credible, resourced investment plan that reduces residual risk over time. That approach aligns to a "so far as reasonably practicable" threshold, where expectations are applied in a way that reflects operational context and avoids holding every entity to identical measures, while still requiring clear rationale for what is treated, what is deferred, and why.

Ensuring effective management of cyber threats impacting national security

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 consider that the most helpful support from government is operational. In particular, sharing of timely threat intelligence, technical incident response assistance, coordination across affected entities, critical information release from affected parties and secure communications channels. For high-severity events, rapid access to necessary capability plus coordinated public messaging to reduce harm and speed restoration would also be of assistance. Support in attaining personnel clearance for staff of CINS is also important.

In addition to the above matters on assistance at the time, it is important that any regime provides clarity about the legal protections for information shared, including safe harbour where appropriate.

Do you think the thresholds for the use of the last-resort power are appropriate? If not, what changes would you propose?

We consider that the thresholds are broadly appropriate if they remain strict, evidence-led, and time-bound. The last-resort power should be reserved for credible national security threats, where voluntary action is insufficient and/or information release is lacking. There should be clear triggers, consultation expectations, and escalation paths.

Additional value may arise from a requirement for post-action review of the use of the power and lessons, where security allows, to build trust and improve readiness.

If this power progresses, it will be important that there is clarity provided of roles in government for overseeing the resilience of each sector, so entities know who their regulator, or point-of-contact, is on these matters.

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 consider that the protections identified are generally reasonable (appeal, review, indemnity, and limits on property acquisition). However, two refinements could strengthen confidence in relation to this power. There should be clear independent oversight of the decision to invoke the power, and clear handling of sensitive information generated during directed actions, are also necessary.

Consideration of a mechanism to address extraordinary costs in rare cases, or at least clarity on what constitutes "reasonable costs" an entity must absorb, is also required.

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

Do you consider that the breaches are appropriately mapped to compliance and enforcement tools? If not, what changes would you propose?

As discussed earlier, we do not consider that offences are an appropriate tool for ensuring compliance and enforcement. Compliance should focus on uplift and learning using guidance, warnings and fines. Punitive action diverts resources away from addressing cyber security risks, towards addressing litigation and the gathering of evidence to address that litigation.

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?

As discussed earlier, we do not support duplicative regulatory regimes. The Discussion Document proposes that there is the ability to obtain a determination that an existing regulator is responsible for ensuring compliance with the cyber security regime. While the suggested approach may have merit, we prefer that duplication of regulatory requirements and enforcement, and compliance requirements is avoided from the outset.

Earlier in our submission, we suggested that exemptions from obligations in the new regime be considered on an obligation-by-obligation basis (rather than entity by entity) basis. If regulatory

regimes and requirements are being duplicated, it may be preferable for the compliance and enforcement regime to be exempted under the cyber security regime.

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, Transpower does not support a punitive regime, as discussed above.

Do you perceive any perverse outcomes as a result of directors being individually liable for the most serious breaches of the regime?

Yes. As discussed above, we consider that resources will be diverted to litigation, rather than timely cyber security risk mitigation, should a punitive regime be imposed.