TCF submission on the DPMC consultation

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

16 April 2026

Introduction

1. Thank you for the opportunity to make a submission on the consultation document *Enhancing the cyber security of New Zealand's critical infrastructure system*. This submission is provided on behalf of the New Zealand Telecommunications Forum (TCF), the industry association for the telecommunications sector. TCF member companies represent over 90 percent of New Zealand telecommunications customers. Our members include network operators, retail service providers and the companies that own and operate cell towers.

2. The TCF supports the development of government policy to lift cyber security across the critical infrastructure system. As digital businesses, our member organisations operate robust cyber security programmes and meet cyber security obligations under the Telecommunications (Interception Capability and Security) Act (TICSA). Sharing information, reporting incidents and having risk management programmes is already standard industry practice. But if the correct balance is not struck between doing the doing, and costly reporting obligations to government, then resources currently dedicated to cyber security may need to be diverted to compliance exercises.

3. Any new cyber security policy and legislative obligations should:

    a. **Be clear about the scope of the critical infrastructure components and operations that will attract obligations, and those that will not.** While we support a principles-based approach to defining critical infrastructure, for this approach to be effective the definition and the associated designation thresholds must be sufficiently clear and tightly scoped. If the net is cast too wide, entities risk diverting resources toward compliance activities instead of focusing effort on the systems and components that are truly critical to service delivery. What is proposed in the consultation document does not provide the necessary clarity or focus - we are not clear on where the boundaries will be set for telecommunications.

b. **Be clear about what good or sufficient practice is under any new regime.** The experience of critical infrastructure entities under the Security of Critical Infrastructure Act (SOCI) is that the Australian Government has been reluctant to provide guidance on what assets are truly critical, the materiality of risks, and the threshold for a relevant impact on an asset. New Zealand should not go down the same path.

c. **Avoid overlapping reporting requirements**. Reporting of incidents, and reporting on compliance with obligations, should be harmonised with existing cyber security related requirements. The telecommunications sector already has network security reporting obligations under TICSA and would expect any new reporting requirements to be streamlined with existing ones. Entities should not have to report to more than one organisation, to minimise regulatory burden and cost.

d. **Take a collaborative rather than a punitive approach, and focus on lifting practice rather than creating a compliance culture.** The Government should continue to strengthen collaboration with industry through mechanisms such as the NCSE-led sector information exchange network, which provide significant resilience benefits without imposing additional regulatory burden.

4. The TCF appreciates DPMC's willingness to engage early in the policy development process, and understands this means the consultation document does not have all the details. If the Government decides to progress this work further we recommend an expert advisory group (across critical infrastructure sectors and government agencies) is established to guide the next stages and design any new standards.

Summary of submission points on proposed measures

Proposal	**Our views**
Definition of critical infrastructure	The definition of critical infrastructure is too broad for telecommunications, because of the reference to essential services. If the definition of essential services from the Emergency Management Bill is relied on, this has the potential to bring a wide range of telecommunications services into scope, when only a subset (such as the 111 service and broadband/connectivity to the prescribed no. of connections) is critical. We recommend: ● Narrowing the definition of critical infrastructure, or being more specific about the meaning of essential services, so it doesn't apply to all telecommunications services. ● A joint government/industry process to clarify which telecommunications services are essential and the thresholds. Australia eventually ran a co-design process to bring the Australian version of TICSA into the SOCI regime, which is reported to have worked well.

Measure 1: information collection by government	Telecommunications network operators and service providers already have reporting obligations under TICSA. If new reporting or information provision requirements are introduced, entities should only have to report once, and not to multiple entities.
Measure 2: voluntary information exchange	Most of our members already voluntarily share information through the Network Operators Group of NCSC's Security Information Exchange network. Creating a larger information sharing group has risks and could constrain the information that members of the group feel comfortable sharing. Two groups (a large and small) could be created to address this.
Measure 3: entities to share certain information with each other	We do not think this aspect is necessary. The focus should be on supporting voluntary information exchange.
Measure 4: incident reporting	● Reporting significant incidents within 24 hours is appropriate, but a full report within 72 hours may not be realistic for major incidents. ● Any new regime should align with existing operational frameworks, using a tiered classification model (detailed on page 6). ● Any new reporting should be aligned with requirements under existing regimes, including TICSA.
Measure 5: risk management programmes	We could support a mandatory requirement to develop a risk management programme based on the five steps in figure four, if: ● this is a process requirement (a regulator cannot substitute or penalise an entity's judgement on which assets are critical, what risks are material, and how much treatment is enough) ● there are limits on the additional measures the minister can prescribe ● there are not administratively burdensome reporting requirements.
Supplier obligations	There is not enough clarity on supplier obligations, including whether: ● critical infrastructure entities that are suppliers to other critical infrastructure entities need to do anything in addition to developing their risk management programme ● suppliers that do not meet the threshold as critical infrastructure entities (e.g. small organisations) have obligations under the regime.
Measure 6: government direction to manage a threat	The use of such a ministerial power must be proportionate and well-justified. It should be informed by expert agencies such as the National Cyber Security Centre and the Government Communications Security Bureau.
Additional obligations	More detail is needed concerning the "enhanced minimum

for critical infrastructure of national significance	requirements" for critical infrastructure of national significance, to give designated entities certainty on their additional obligations.
Enforcement (criminal sanctions)	While cyber security is a governance-level responsibility, criminal liability is disproportionate to directors' control over operational risks and may deter qualified individuals from governance roles. It could also lead to overly risk-adverse decision making.

Defining critical infrastructure

5. If new obligations are going to be introduced concerning the cybersecurity of critical infrastructure, it is necessary to have a shared understanding of criticality. If critical infrastructure is defined too broadly, then everything will be critical and government agencies and critical infrastructure entities will be overwhelmed with requirements and reporting. It will also mean that critical infrastructure entities can't focus on the systems that are truly critical to operations. For telecommunications, examples of critical systems and services include emergency calling capability, core voice and messaging services necessary for public safety, interconnection and core network functions required to maintain national connectivity.

6. The Australian experience has been that critical infrastructure was defined too broadly. Submitters to the SOCI review highlighted the very broad definitions of assets, data storage systems and critical workers. Australian critical infrastructure entities have called for clarity on which infrastructure assets, systems and services are critical, and which are not.

7. The proposed definitions in the consultation document take a similarly broad approach, and as a result leave the sector unsure what its obligations would be if New Zealand implemented a similar regime for cyber security. While we support a principles-based approach to defining critical infrastructure, for this approach to be effective the definition of critical infrastructure and the associated designation thresholds must be sufficiently clear and tightly scoped.

8. Of particular concern is the relationship between "critical infrastructure" and "essential services". The definition of critical infrastructure includes components that provide essential services. Two of the proposed obligations reference essential services: entities must identify the components critical to the delivery of essential services, and report on significant cyber incidents likely to have a serious impact on the delivery of essential services.

9. The meaning of "essential services" is therefore very important to understanding potential obligations. Officials have indicated that the definition of essential services in the Emergency Management Bill would apply. The definition in clause 7 of Bill is intentionally broad and designed for an emergency management context, but it is not suitable as a trigger for ongoing cybersecurity obligations applied through a threshold-based regime.

10. We submit that essential services would need to be more precisely defined (or supplemented with limiting criteria) in any new cyber security regime. This would provide necessary regulatory certainty about what is in scope and what is not, and enable entities to focus on the systems that are genuinely critical. We recommend a joint telco industry/government process to work through the essential services question.

Proposed thresholds for communications

11. Thresholds would be a useful initial screening tool but should not automatically deem all assets or services of an in-scope entity to be critical.

Proposals re information exchange (measures one to three)

Measure one: providing information to the government

12. The regulations should not allow broad open-ended data collection processes. The information able to be collected should:

    a. be limited to what is necessary for national risk management

    b. minimise repeat requests where information is already held elsewhere

    c. avoid duplicative technical inventories

    d. be targeted, proportionate and risk based.

13. Telecommunications network operators and service providers already have reporting obligations under TICSA. If new reporting or information provision requirements are introduced, entities should only have to report once, and not to multiple entities.

Measure two: voluntary information exchange

14. Some of our members already voluntarily share information through the Network Operators Group of NCSC's Security Information Exchange network.

15. While we support the intent of requiring further information exchange, it needs to be carefully considered. Creating a larger information sharing group has some risks and could constrain the information that members of the group feel comfortable sharing.

16. On the other hand we can also see value for smaller telcos (who do not meet the 10 000 customer threshold) being able to participate in an information sharing process. Clarity would be needed on whether entities that do not meet the thresholds would be able to participate.

17. The balance between security and sharing could perhaps be addressed by having two groups (one larger and a smaller group for critical infrastructure of national significance), as has been done in Australia.

Measure three: requiring the sharing of certain information

18. We do not think this aspect is necessary. The focus should be on supporting voluntary information exchange.

Reporting cyber incidents (measure four)

19. Measure four proposes regular reporting of all cyber incidents, and reporting of "significant cyber incidents" "as soon as practicable". An initial early warning within 24 hours of detection, and a full report no later than 72 hours post detection is suggested in the discussion document for significant incidents.

20. We agree that timely reporting of significant cyber incidents is important for national situational awareness. However, in telecommunications environments, large volumes of security alerts and anomalous events occur daily as part of normal network operations. If any new reporting requirements did not appropriately distinguish between routine security activity and incidents that are materially significant, there is a risk that routine security activity may unintentionally become reportable, creating unnecessary administrative overhead without improving national situational awareness.

21. This outcome could be avoided by:

    a. Aligning the definition of cyber incidents with existing operational frameworks used by critical infrastructure providers, and definitions in existing legislative requirements, such as the Privacy Act breach notification processes.

    b. Using a tiered incident classification model, distinguishing between:

        i. Cyber events (alerts or anomalies) - no requirement to notify

        ii. Cyber incidents (confirmed compromise or operational impact) - periodic aggregated reporting

        iii. Significant cyber incidents (material impact to critical services or sensitive data) - early notification in 24 hours to enable government situational awareness and potential coordinated response.

22. Reporting of significant incidents (with high level situational information) within 24 hours is appropriate. However, a requirement to provide a full report within 72 hours may not be realistic for major incidents. In practice, complex cyber incidents can remain under active investigation for days or weeks while containment, recovery and forensic analysis takes place.

23. Reporting obligations and timelines will need to be able to be adjusted to address the situation where an incident is initially assessed as potentially significant but is later determined to have lower impact, and vice versa.

24. It is also necessary to be clear about the essential services that would be the threshold for determining if an incident is significant (the discussion document suggests a significant

incident is one that has or is likely to have a serious impact on the delivery of essential services). We explain this issue in the section of our submission on defining critical infrastructure.

Developing cyber security risk management programmes

25. It is already industry best practice to have a cyber security risk management programme, and to align with internationally recognised frameworks and standards such as ISO 27001 and NIST CSF.

26. The TCF could support a mandatory requirement to have a cyber security risk management programme, based on the five steps in figure four on page 16 of the discussion document, if:

    a. It is a process requirement (a regulator could not substitute its judgement for that of a critical infrastructure entity on substantive matters)

    b. There are guard rails on the proposed ability for the responsible minister to specify any additional measures entities may need to take as part of a risk management programme, or to require entities to take prescribed actions to manage a specific risk or set of risks. For example, the responsible minister should not be able to specify these requirements unless following advice from NCSC

    c. Reporting obligations are not administratively burdensome

    d. The requirement concerning international frameworks is to align, but not follow in all respects, as these frameworks are not always a complete fit for all sectors.

Demonstrating and determining compliance with the minimum requirements for risk management programmes

27. The consultation document considers a range of options for demonstrating compliance, ranging from director attestation (but not third party audit), a short report documenting how requirements have been met, and the possibility of the regulator later being able to act on the information in that report. The intention seems to be to start off light touch and to eventually have a full compliance tool box, and the possibility of a regulator being able to substitute its judgement for that of a critical infrastructure entity.

Director attestation

28. If director attestation is required then directors are likely to require an external audit (especially if there is director liability). As noted at consultation hui, external audits are unlikely to enhance cyber security, but are likely to benefit consulting firms.

29. An alternative approach could be to require attestation (of the process requirement) by appropriately qualified persons working for the entity.

Who makes the final calls about the substance of a cyber security risk management programme?

30. It is not clear to us, from the consultation document, who would make the final decisions on the substantive matters in a risk management programme, and whether the components,

risks and treatments identified are the right ones. Options could include the entity, the regulator or a third party auditor.

31. Our view is that entities are best placed to assess the risks affecting their operations, and need flexibility to determine the appropriate treatments. Making these calls at the entity level would be consistent with comments made at the consultation hui about the risk management minimum standard being a process requirement, and government not having the necessary expertise. But it was also suggested that government could use information in the "short report" about the risk management programme to determine if intervention was needed. The discussion document also says that the responsible minister could specify additional matters that need to be undertaken as part of a risk management programme.

32. It should be explicit that the risk management programme minimum standard is a process requirement. More specifically, it should be clear that the regime does not require certification, the achievement of certain maturity levels, or the conversion of risk frameworks into audit checklists. This will enable alignment with international standards while retaining necessary flexibility to address any entity specific risks.

Obligations of suppliers to critical infrastructure

33. The consultation document notes that entities such as suppliers, that have operational control over critical components, would be required to support critical infrastructure entities as far as practicable. No information is provided on what sort of support might be required.

34. TCF members are interested in this requirement from three perspectives:

    a. As suppliers of services to other critical infrastructure entities. Is there a need to meet two or more sets of requirements, one as a critical infrastructure entity and additional requirements to support critical infrastructure entities who are customers and line up with their risk management programmes?

    b. As telecommunications suppliers to critical infrastructure entities or critical infrastructure entities of significance, who don't meet the 10 000 customer or connection threshold so are not critical infrastructure entities themselves. Would these smaller telcos be pulled into the regime by virtue of their client's critical infrastructure status?

    c. As customers of suppliers. How far do we have to go to ensure we have the necessary support of our suppliers, especially where they are international suppliers with a standardised offering?

35. Clarity is sought on these questions. In relation to question (a), during one of the consultation hui it was explained that if a critical infrastructure entity has a risk management programme that meets the standards required for critical infrastructure entities, it does not have to meet additional requirements as a supplier to another critical infrastructure entity. We submit this would need to be legislated for.

36. In Australia there have been different interpretations about the obligations of suppliers, which supports the need for clarity on supplier issues. Guidance with examples would be useful.

A last resort power for the minister (measure six)

37. Measure six would grant the responsible minister the power to direct a critical infrastructure entity to do, or refrain from doing, anything necessary to manage a cyber threat for national security reasons.

38. While the discussion document suggests some natural justice safeguards, it doesn't provide any information about the sorts of things a minister could require. The words "anything necessary" are too broad.

39. Any reserve power should be:

    a. clearly limited to exceptional circumstances

    b. exercised only on the basis of technical advice (e.g. from the National Cyber Security Centre and the Government Communications Security Bureau)

    c. subject to statutory safeguards including necessity, proportionality, defined duration and review mechanisms.

Additional obligations for critical infrastructure of national significance

40. The discussion document indicates (on page 17) there would be "enhanced minimum requirements" for critical infrastructure of national significance, but there is limited information on what these additional obligations would entail. Any additional obligations would need to be clarified ahead of time, not left to regulator or ministerial discretion, to give designated entities certainty on what will be required of them.

Criminal penalties

41. The consultation document discusses the possibility of criminal sanctions for organisations and directors. We are of the view this could lead to unintended consequences, including:

    a. encouraging a compliance culture that shifts focus towards regulatory compliance instead of cyber security uplift

    b. diverting funds tagged for cyber security capability and resilience to paying fines

    c. encouraging overly risk-averse governance behaviour that may slow innovation and operational decision making - this would likely include insistence on external auditing (something DPMC does not think would add value)

    d. reluctance among experienced professionals to serve as directors of critical infrastructure organisations.

42. Policy to introduce criminal liability for directors in cyber security would be at odds with recent government decisions to significantly soften or remove forms of director liability in other regulatory systems, including under the Credit Contracts and Consumer Finance Act, the climate related disclosures regime and in health and safety. The goal of these reforms has been to reduce compliance heavy burdens and prevent directors from becoming overly risk-averse or focused on tick-box exercises at the expense of strategic governance. We also note the Law Commission is undertaking a review of directors' duties and liabilities.

43. While we do not support criminal liability, we think it is appropriate to require directors to demonstrate reasonable oversight of cybersecurity risk.

Potential compliance costs

44. We anticipate substantial compliance costs for telecommunications network operators, based on the experience of Australian telcos with the cyber security aspects of SOCI. These costs have included:

    a. administrative reporting on compliance with requirements, with significant regulatory duplication

    b. aligning existing risk management programmes with prescribed standards

    c. retrofitting security controls into old architecture creating capital expenditure requirements that were not part of the original TSSR (Telecommunications Sector Security Reforms) baseline

    d. supply chain auditing (checking vendors meet security standards) has added significant legal and procurement overheads, estimated at five to ten percent of contract values

    e. direct fees and administrative costs for background checks for the broadly defined category of "critical workers".

45. The updated Australian regulatory impact analysis estimated a total average regulatory cost at $9m per entity to transition to the full SOCI risk management programme framework. With an average annual ongoing cost of 4.1 million per entity (see supplementary analysis for Critical Telecommunications Assets - page 12).

Closing remarks

46. If there are any questions about this submission please contact kim.connolly-stone@tcf.org.nz in the first instance.