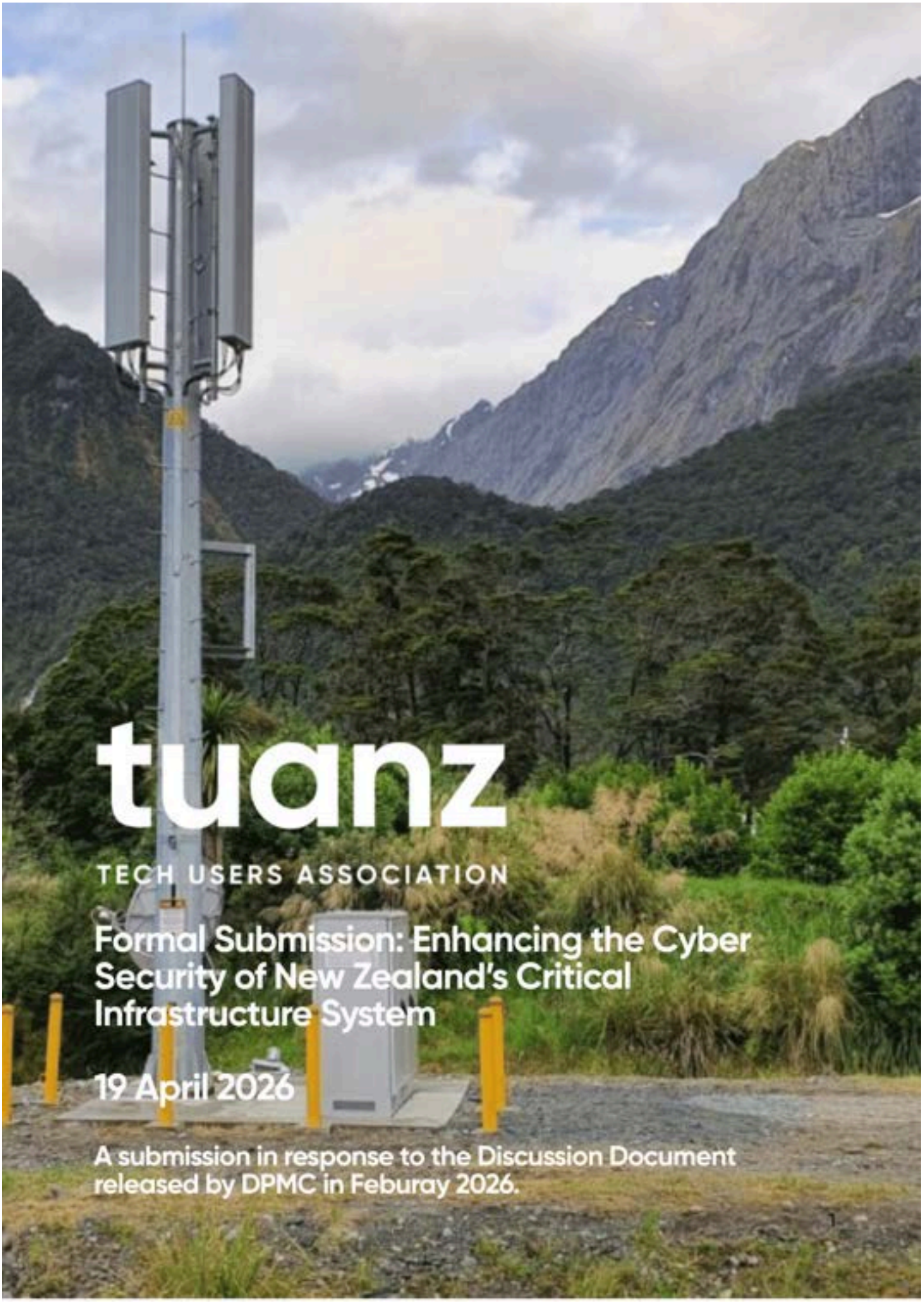

tuanz

TECH USERS ASSOCIATION

Formal Submission: Enhancing the Cyber Security of New Zealand's Critical Infrastructure System

19 April 2026

A submission in response to the Discussion Document released by DPMC in Feburay 2026.

1. Introduction and Strategic Context

As the only truly independent association representing the users of technology in New Zealand (TUANZ), we are pleased to present this formal submission regarding the *2026 Cyber Security Discussion Document*. This submission represents the collective voice of New Zealand technology users and is framed by our association's 40-year milestone (1986–2026) as an independent advocate. In an environment where digital connectivity is the "lifeblood" of our economy and society, the resilience of our critical infrastructure is not merely a technical requirement but a strategic national security imperative.

The purpose of this document is to provide a user-centric perspective on the government's proposed framework. Our contribution is grounded in the TUANZ philosophy that cyber security and online safety are public goods. Just as the state provides physical safety through roads and policing, it should ensure a safe digital environment. We assert that the era of "user beware" must end; the complexity of current threats necessitates proactive government leadership over reactive strategies. This submission critiques the proposed framework and provides a detailed response to the government's specific consultation queries.

2. General Comments: The State of Aotearoa's Digital Resilience

New Zealand has moved beyond isolated technical vulnerabilities into a period of automated, AI-driven social engineering at scale. Threat actors, such as the PRC-affiliated **Salt Typhoon** (targeting telecommunications for espionage) and **Volt Typhoon** (infiltrating energy and transport systems), demonstrate that our infrastructure is under active, sophisticated observation. Furthermore, incidents like the **Manage My Health** breach, affecting 126,000 New Zealanders, highlight the devastating impact of supply chain vulnerabilities.

TUANZ identifies three critical failures that the 2026 framework must resolve:

1. **The Cyber Equity Gap:** A dangerous divide exists between large corporates and Small to Medium Enterprises (SMEs). Currently, 35% of small organisations report that their resilience is insufficient—representing a staggering **seven-fold increase** since 2022.

2. **Fragmented Regulation:** There is a strong perception of uncoordinated government strategy. Leaders are frustrated by a landscape of fragmented, voluntary initiatives. Resilience requires a move from advisory guidance to enforceable standards.

3. **The Burden on the User:** With $200 million in reported losses to scams in the year to September 2024, it is clear that relying on individual vigilance is failing. When threats are structurally embedded, the safety nets—such as platform accountability and bank reimbursement—remain inadequate.

3. Comprehensive Response to Consultation Questions

This section provides our responses to the government's queries, grounded in the TUANZ Cyber Security Community's expert deliberations. These responses prioritise a balance between operational efficiency and the protection of the end-user.

Consultation Question	TUANZ Formal Response
Defining critical infrastructure: Would you support the proposed approach to defining critical infrastructure and critical infrastructure of national significance?	**Support Principles-Based Approach.** TUANZ supports the proposed definition. We believe it creates the necessary certainty for both providers and the public.
Do you consider any essential services have been included or excluded that should not be?	**Comprehensive Inclusion.** The seven identified essential services (Communications, Energy, Finance, Health, Transport, Water, Defence) are appropriate. However, we must ensure "Cloud Computing" is strictly categorised as an essential dependency.
Do you think the example thresholds for defining critical infrastructure have been set appropriately?	**Support Identified Thresholds.** We generally support the **Telco Threshold** of 10,000+ customers but recommend that this be reviewed in the next review of this strategy to reflect any market changes.
Are there other factors to consider in assessing "National Significance" (CINS)?	**Interdependency Mapping.** Beyond consequences, the Minister must consider "downstream impact." Disruption to a smaller provider that supplies data processing to a CINS entity must be considered in the designation.
Do you agree that the Minister responsible should have the ability to designate or exempt entities?	**Ministerial Oversight.** We agree, provided a statement of reasons is tabled in Parliament. Flexible designation is required for entities that fall below thresholds but possess high systemic interdependency.
Information Sharing: Do you agree with the proposed approach to protecting the data shared?	**Enforceable Confidentiality.** We support the approach, provided that a breach of protection by a government agency is an enforceable offense to maintain industry trust.
What effect would all essential providers participating in a formal exchange have on your willingness to participate?	**Exchange Participation.** TUANZ supports broad participation in a formal exchange, provided there are clear legal protections, trusted governance, and tangible value for participants through shared intelligence and coordinated response
How frequently should regular reporting of all cyber incidents be required?	**Quarterly Reporting.** TUANZ supports a quarterly cadence for general incident data to build a common operating picture without overburdening resources.

Does the proposed definition of a "cyber incident" fit your enterprise risk management?	**Support Alignment.** We support a broad definition. However, the focus must remain on the **Impact on Essential Services** rather than just technical anomalies.
Would a requirement to report significant incidents make you less willing to report voluntarily?	**Support Mandatory Reporting.** TUANZ rejects the idea that mandatory requirements stifle voluntary sharing. In fact, a clear regulatory mandate often provides the "safe harbour" legal teams require to share data.
Are the criteria of "serious and above" for 72-hour reporting appropriate?	**Mandate Transparency.** Support the 72-hour window. However, we insist on a **Consumer Notification** requirement; reporting to NCSC provides government visibility but leaves the impacted tech user in the dark.
What impact could the requirement to report significant incidents have on response processes?	**Process Integration.** While it may initially increase legal involvement, clear standards will eventually streamline responses, provided reporting is to a single, centralised window (NCSC).
Minimum Risk Management: Are specific words proposed for risk management (p.15) likely to conflict with existing processes?	**Ecosystem Alignment.** We do not see conflict, provided the NCSC allows entities to build upon existing ISO 27001 or NIST CSF frameworks rather than inventing "New Zealand-only" technical terms.
Should "Critical Components" align with the emergency management system?	**Support Alignment.** Consistency between the Emergency Management Bill and this framework is essential for operational clarity during a national crisis.
Can "Material Risk" be given effect within existing enterprise risk management?	**Expert Judgment.** We support the "reasonable person" test for materiality. This allows businesses to prioritise the threats most likely to cause cascading failure.
Should the threshold for treating risks be set at "so far as reasonably practicable"?	**Practical Resilience.** We support this language. It recognises that absolute security is impossible and focuses on mitigating the most impactful threats within operational constraints.
Do you support complying with a cyber security framework endorsed by the NCSC?	**Support Shared Responsibility.** TUANZ supports alignment with international frameworks. We suggest the **Essential Eight** or **UK 10 Steps** as an accessible baseline for smaller entities within the system.
Should government prescribe which international frameworks are acceptable?	**Flexible Standards.** No, the government should not prescribe a single framework but should provide a "pre-approved list" to reduce compliance confusion.

Is the requirement for third-party vendors to support responsible entities important?	**Supply Chain Accountability.** This is critical. Major incidents like **Manage My Health** prove that critical infrastructure is only as strong as its third-party vendors. Support this requirement.
Are there alternative ways to recognise equivalent regulation?	**Outcome-Based Determination.** We support the regulator issuing "determinations" for sectors like banking (RBNZ) or border security (Customs) where equivalent standards already exist.
Is there a more effective way to ensure compliance than individual director responsibility?	**Director Accountability.** TUANZ supports individual director liability for serious breaches. Board-level attention is the only way to ensure cyber risk is treated as a core business risk.
How should entities demonstrate compliance?	**Attestation to Report.** A staged approach: initially a formal declaration (attestation), moving toward short reports. Third-party audits should be a last resort due to cost.
National Security Threats: What government support is most helpful for restoration?	**Operational Intelligence.** Direct NCSC technical support and community-based support models to help users navigate the social engineering aspects of the crisis are most helpful.
Are the thresholds for the use of the "Last-Resort Power" appropriate?	**Support National Security.** We support these powers as a last resort, provided adequate consultation occurs and indemnity against legal liability is provided to the entity.
Are protections for entities subject to last-resort powers appropriate?	**Natural Justice.** Support the ability to appeal to the Minister and statutory review. These are essential to prevent executive overreach.
Mandatory Requirements: Are breaches appropriately mapped to compliance tools?	**Proportionate Enforcement.** We support the mapping. Targeted education should be the first step, with criminal penalties reserved for "negligent, reckless, or knowing" failures.
How should breaches across two or more regimes be managed?	**Avoid Double Jeopardy.** The more stringent penalty should apply. Cooperation between regulators (e.g., NCSC and Commerce Commission) is non-negotiable.
Should penalties apply to directors as well as the organisation?	**Balanced Support.** Yes, but we highlight the **Pricing Flow-on Effect.** Compliance costs for directors will likely flow into retail pricing, impacting consumers who fall below the 10,000-customer threshold.

Do you perceive perverse outcomes from individual director liability?	**Risk Aversion.** Potential for directors to avoid the sector. However, the risk of underinvestment in national resilience is far more "perverse" and dangerous to the public.

4. Critical Synthesis: "What is Missing" from the Proposed Framework

While the discussion document is a significant step forward, the TUANZ committee identifies three strategic omissions:

- **The Lifespan Human Firewall:** The current proposal focuses heavily on technical infrastructure and schools. However, cyber threats like those seen in the $200m scam losses target behavior across all age groups. We argue for a **"lifespan" approach** that includes adult capability building and community-based support models. Human capability should be recognised as a core component of national cyber resilience, alongside technical and organisational controls. Protecting the infrastructure is only half the battle; we must develop the human firewall where people actually live and work.

- **Pricing and Compliance Flow-on Effects:** The document suggests that compliance costs for regulated entities can be offset by revenue. TUANZ notes a critical "So What?" for the consumer: these costs will flow into wholesale and retail pricing. This creates a disproportionate burden on smaller retailers and consumers who pay higher prices driven by the compliance of larger providers but receive no direct regulatory protection.

- **Consumer Notification Gaps:** Reporting to the NCSC ensures government visibility but does not mandate transparency for the impacted user. We believe that if a tech user's data is compromised by a critical infrastructure provider, **mandatory consumer notification** must be a requirement of the framework.

5. Conclusion and Call to Action

The path to a resilient Aotearoa requires a "whole-of-ecosystem" approach led by the government. We cannot secure our infrastructure by technical patches alone; we must address the systemic inequities—particularly the **SME Cyber Equity Gap**—that our adversaries exploit.

New Zealand's economic prosperity depends on a digital environment where trust and safety are guaranteed, not optional. TUANZ remains committed to working with the government to ensure this framework protects every technology user in Aotearoa.

TUANZ: Championing a Brighter Digital Future for every New Zealander

The Technology Users Association of New Zealand (TUANZ) is the voice of technology users in Aotearoa New Zealand. Established as a not-forprofit organisation, TUANZ acts as the independent group representing the interests and needs of individuals, businesses, and organizations as they navigate the evolving technology landscape.

Our membership encompasses a diverse range of technology users, from small businesses and innovative startups to large enterprises and public sector entities. This broad network connects those who utilise technology to achieve their goals, fostering a community dedicated to understanding, adopting, and maximising the benefits of digital tools and services.

TUANZ plays a crucial role in bridging the gap between technology providers and end-users. We work collaboratively across sectors, engaging with government, industry, and the wider community to ensure that technology deployment and policy decisions are user-centric and contribute to a thriving digital ecosystem for all New Zealanders.

Our focus is on empowering technology users through education, advocacy, and the facilitation of meaningful connections. We strive to ensure that New Zealanders can confidently and effectively leverage technology to enhance productivity, innovation, and overall quality of life. We provide a platform for an informed and influential user voice, advocating for policies and practices that support positive technology outcomes for our members and the nation.


tuanz
TECH USERS ASSOCIATION
2026