20 May 2025

Emergency Management Reform Submission

National Emergency Management Agency

Table of Contents

Introduction

InternetNZ | Ipurangi Aotearoa manages the .nz DNS (DNS), a vital part of the Internet's structure. It supports the DNS resolution process, converting human-readable domain names (e.g., civildefence.govt.nz) into machine-readable IP addresses and other references. InternetNZ's DNS infrastructure emphasises fault-tolerance and resilience, featuring redundancy across diverse locations and active monitoring to address anomalies.

InternetNZ is an independent organisation that operates within multistakeholder Internet governance frameworks, using internationally agreed-upon standards for Internet management.

Since 1995, we have held the delegation for the ccTLD (country code top-level domain) from the Internet Assigned Numbers Authority (IANA). InternetNZ also has a Memorandum of Understanding with the Ministry of Business, Innovation and Employment (MBIE). These arrangements confirm InternetNZ's role of operating the .nz and managing a stable and secure .nz DNS in service to and for the benefit of New Zealand's internet community.

Summary of Submission

InternetNZ's role is narrowly scoped to maintaining the .nz ccTLD — a function already resilient through global partnerships and redundancies. Any regulation must account for the full chain of dependencies (ISPs, energy suppliers) to avoid gaps in emergency readiness.

InternetNZ notes that the potential scope of new essential infrastructure providers includes the operation of the DNS, including the management of New Zealand's ccTLD.

New Zealand's DNS has never been impacted by natural hazards or emergency management events. While we provide critical infrastructure on behalf of New Zealand's communities, we do not believe that we need to be designated as an essential service under the Civil Defence Emergency Management Act, or that ccTLD operations should be subject to essential service obligations.

We think assigning an essential service classification to the ccTLD is not necessary for emergency management purposes, and any obligations must be precisely scoped and proportional to the distinct technical function and operational parameters of a ccTLD operator. This would require explicit safeguards to prevent the misapplication of grouping New Zealand's ccTLD operations within broader telecommunications sector requirements that are designed for other providers whose operational realities and abilities differ greatly from those within InternetNZ's mandate.

InternetNZ's DNS role operates within internationally coordinated technical standards and multistakeholder governance frameworks, which differ fundamentally from the operational models of physical infrastructure providers and differ considerably from national and regional provision of essential services.

InternetNZ does not receive any Crown funding. Therefore, in a situation where there are legislatively mandated obligations for emergency management, additional funding will be required for us to effectively meet those requirements.

We would welcome the opportunity to discuss in more detail the operational nature of the DNS and ccTLD, and how our unique position within New Zealand's critical infrastructure and essential services might be better reflected within the strengthening of New Zealand's National Emergency ecosystem.

NEMA reform objectives for CDEM Act

The Government has five proposed objectives for change. InternetNZ's submission substantially focuses on three of those objectives:

- strengthening community and iwi Māori participation
- enabling a higher minimum standard of emergency management
- minimising disruption to essential services

Objective 1: Strengthening community and iwi Māori participation

Digital Equity and Emergency Access

Recent emergency events have highlighted persistent digital equity challenges that extend beyond the core service that InternetNZ runs of DNS availability. Our latest Internet Insights report indicated that 39% of New Zealanders surveyed are very or extremely concerned about being cut off from the Internet for a period of time. 62% of New Zealanders surveyed were concerned that people from lower socio-economic backgrounds may have limited access to the Internet[1].

InternetNZ supports the kaupapa of many community or charitable organisations focused on addressing digital equity. Equitable access to communications during an emergency requires addressing last-mile connectivity (e.g., rural broadband, ISP redundancy), but also ensuring that emergency communication systems are available and accessible to everybody regardless of geographic location or socio-economic status.

Our preference would be for the suggested option (Issue 1: Option 4) where the broad and diverse needs of communities and iwi Māori are explicitly included in legislation for national-level emergency management arrangements. This would ensure that levels of digital access are able to meet the needs of both responders and communities in times of distress. In particular, we recommend consideration under Issues 2 & 4 to explicitly outline the need for ongoing connectivity and emergency communication systems to be funded and implemented into all community centres or marae that support the critical emergency management centre network.

[1] InternetNZ Internet Insights 2024
https://internetnz.nz/assets/Archives/New-Zealands-Internet-Insights-2024.pdf

Objective 3: Enable a higher minimum standard of emergency management

We believe DNSs should not be in scope for emergency management regulatory frameworks. Mostly because different obligations should apply for utilities that are first responders to natural hazards or in an emergency, and the networks that need to be working.

Key problem: the Director's mandate to set expectations and monitor performance

InternetNZ thinks that while strengthening the Director's mandate may lead to clearer expectations, that whatever option is chosen should not take a blanket approach (ie, including DNS as part of the broader telecoms sector) as that may create unintended consequences and burden of requiring additional monitoring, reporting and oversight that is not warranted for DNS operations in emergency responses. To that end, our preference would be for non-legislative approaches such as guidance and strengthened governance.

We understand that NEMA is still considering the range of people and organisations to be captured (as per para 117). Our assessment is that InternetNZ should not be captured within the definition or responsibilities of lifeline utilities because these obligations are more suited to essential services that are first responders in an emergency.

We also note the suggested strengthening of the mandate to intervene and address performance issues. To avoid creating ineffective or counterproductive policy outcomes, account must be taken of the global and interdependent nature of DNS operations, and that InternetNZ already meets multiple global obligations in order to be the ccTLD manager for .nz. For example, we have existing obligations under RFC1591 [https://www.rfc-editor.org/rfc/rfc1591.html]

We note there is a higher minimum standard for obligations that includes Cloud services and DNS but do not believe that higher level of obligation is warranted during natural hazard emergencies, or similar to those that would apply for telecoms. Again we point out the risk to .nz during an emergency management is extremely low and different to those experienced by telecoms because DNS operations have always remained working during an emergency.

Unintended consequences on New Zealand's domain name market

The DNS is global and additional compliance costs in the New Zealand domain name ecosystem presents considerations that warrant noting. Current data indicates that while 75% of New Zealand businesses use a domain name, 70% of those use .nz. Should emergency management regulations or obligations place a considerable financial burden on the operation of the .nz ccTLD, the regulatory imbalance could inadvertently disadvantage locally operated namespace providers, including both .nz and other New Zealand-based domains such as .kiwi.

Any additional legislative obligations, particularly in cybersecurity, would impose resource pressures and require additional funding in order to meet standards that might be set by an updated CDEM Act.

If InternetNZ was assessed to be responsible for a lifeline utility, our ability to meet any new regulations and obligations may significantly exceed our revenue. We would welcome discussion with officials on how these national responsibilities are to be resourced and any impact managed.

Objective 4: Minimise disruption to essential services

Creating clear definitions and scope of critical infrastructure, essential services and lifeline utilities would help to create certainty for providers on their roles within the ecosystem.

Key problem: narrow definition of "lifeline utility" in the CDEM Act

InternetNZ does not believe DNSs should be included in any expanded definition of a "lifeline utility". We would not favour the DNS being included in a lifeline utilities framework that provides for classes of organisations to be recognised as "essential infrastructure provider" or "essential services" due to the unique nature of our business. We recognise that connection is critical in an emergency situation, but DNS operations are not needed as an on-the-ground first response in most emergencies. The DNS ecosystem is inherently inter-dependent, and within our scope, .nz has a high degree of operational resilience, with multiple layers of redundancy and caching that already mitigates most localised disruptions.

Since 1995, InternetNZ (and previous entities) have been committed to consistent reliability. Only one significant partial outage has occurred over the last 30 years. This incident has been independently reviewed, and lessons learnt have improved our processes and procedures and informed other global DNS providers.

The .nz DNS is resilient by design, with 30 years of near-continuous uptime. However, its effectiveness in emergencies depends on broader infrastructure stability. For example, during the 2023 DNSSEC incident, cached DNS responses prevented widespread outages, but some users still lost access due to localised ISP or device-level issues.

The .nz DNS infrastructure's design directly supports emergency resilience through multiple technical and operational safeguards. During emergency situations, the system's 1-day DS record (Delegation Signer record) Time to Live (TTL) would ensure that emergency services domains remain accessible for at least 24 hours without requiring cache updates, while the 7-day cryptographic signature validity maintains verification continuity through extended outages. The dual-signer architecture with geographically separated HSM's (Hardware Security Modules) provides physical disaster protection, allowing immediate failover if one location becomes compromised. Automatic ZSK (Zone Signing Key) rotations every 90 days

create regular recovery opportunities, preventing single points of failure from becoming permanent vulnerabilities.

The May DNSSEC 2023 incident demonstrated these safeguards in action — despite the validation errors, domains remained resolvable for non-validating queries, and the 5-day buffer built into the TTL structure provided largely uninterrupted access while technical teams implemented solutions. Post-incident improvements now enforce stricter consistency checks between configured and published TTL values, while maintaining the overlapping validity periods that ensure emergency services retain both accessibility and authentication capabilities even during prolonged system disruptions. This architecture specifically addresses the dual requirements of emergency scenarios: immediate access continuity through cached records when systems are stressed, and cryptographic verification integrity when establishing trusted communications channels is critical.

InternetNZ applies these rigorous technical and operational standards, including regular operational integrity checks (e.g. zone file validation and change detection monitoring), business continuity procedures reviewed in 2023, and advanced threat mitigation controls such as DDoS protection, multi-factor authentication, and logical network segmentation.

Key problem: Inadequate business continuity planning

InternetNZ would not want to see increased levels of oversight from the Director of NEMA or greater obligations and compliance for business continuity or emergency response planning. Most sectors already have their own sector or industry contexts which would make oversight or consistent BCP planning challenging to monitor. We also note that we already have to meet global internet protocols, policies, and standards as the assigned ccTLD for New Zealand.

Similarly, the need to participate in planning at the regional or national level may not be possible for InternetNZ because of the pressure it would place on our small specialised workforce.

Our preference would be that existing groups or mechanisms that are already effective such as the Telecommunications Emergency Forum (TEF) are leveraged rather than new organising structures created. InternetNZ actively participates in sector-wide emergency preparedness initiatives through the TEF. We regularly contribute to cross-sector exercises and planning activities specifically designed to strengthen coordinated responses across New Zealand's critical infrastructure providers.

For InternetNZ specifically, our business continuity and disaster response plans contain similar planning scenarios and are consistent with those illustrated in the discussion document. In almost all scenarios, the DNS can continue to operate due to the built-in redundancy of our infrastructure, which spans multiple regions within Aotearoa and globally distributed partner sites. We also employ layered mitigations, including penetration testing, configuration monitoring, and robust failover mechanisms.

The ability of InternetNZ's registry to resolve DNS queries during emergencies will always depend on the functioning of the network, telecommunications, and data centre operators. But the global DNS system maintains continuity during localised outages, in part due to recursive DNS caching in combination with redundant network design, which are services operated by both local and international organisations.

Key problem: duty to use or disclose information

As above, if there are legislated expectations around the roles and responsibilities to participate in CDEM Groups, we believe this would need careful consideration for smaller entities such as ourselves, and our ability to participate. We would prefer that existing mechanisms that work well, such as TEF, remain.

Concluding Recommendations

InternetNZ submits the following recommendations for NEMA's consideration:

1. Any classification of essential services under the Civil Defence Emergency Management Act should carefully delineate between essential services and emergencies — some are required to restore services to people (telecoms) and some are unlikely to have been disrupted (DNS). The DNS operates fundamentally differently from physical infrastructure providers, serving as a coordination layer into the global internet rather than a delivery mechanism. This distinction warrants specific definitional clarity to ensure regulatory frameworks align with technical realities.

2. Effective emergency preparedness requires the recognition that InternetNZ already plays a specialised role of ccTLD operator within the broader telecommunications ecosystem. InternetNZ's function as steward of the .nz namespace has a unique, and narrowly-scoped mandate that operates within global technical standards and governance frameworks. Policy approaches need to preserve this specialised character while addressing emergency resilience through appropriate, targeted measures.

3. Resilience planning should focus on points of greatest systemic vulnerability for New Zealand's communities. DNS architecture's distributed nature inherently provides substantial redundancy by design, as demonstrated by .nz's 30-year operational history. Regulatory efforts may achieve greater impact by concentrating on infrastructure components where single points of failure actually exist.

4. InternetNZ would be happy to provide specific technical expertise to inform our classification and role within New Zealand's emergency management system.

InternetNZ would appreciate the opportunity to discuss the specific points we have raised in our submission with NEMA. Please contact policy@internetnz.net.nz.