19 April 2026

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

Via email: criticalinfrastructure@dpmc.govt.nz

ERGANZ SUBMISSION ON ENHANCING CYBER SECURITY

The Electricity Retailers' and Generators' Association of New Zealand ('ERGANZ') welcomes the opportunity to provide feedback on the Department of the Prime Minister and Cabinet's discussion paper, 'Enhancing the cyber security of New Zealand's critical infrastructure system' from February 2026.

ERGANZ is the industry association representing companies that generate and sell electricity to Kiwi households and businesses. Collectively, our members supply almost 90 per cent of New Zealand's electricity. We work for a competitive, fair, and sustainable electricity market that benefits consumers.

Summary

ERGANZ supports the Government's objective of lifting the cyber security posture of New Zealand's critical infrastructure system. The threat environment has evolved, the interdependencies between sectors have deepened, and the consequences of a successful attack on any one part of the electricity system extend well beyond the affected participant. Our members take cyber security seriously, invest materially in it, and engage constructively with the National Cyber Security Centre through existing voluntary mechanisms.

We recognise that New Zealand's current voluntary approach has limitations and accept that a calibrated, legislative uplift can be justified. However, the measures as proposed require some refinement before they deliver proportionate benefit. Our principal concerns are:

- Duplication with existing electricity sector regulation. The industry is already heavily regulated by the Electricity Authority and the Commerce Commission, and the Authority's current work programme already includes significant digital components. Any new regime must align with and build on, rather than duplicate, existing obligations. The arrangements should also:
    - adopt a "report once" principle to streamline process and reduce complexity; and

    - remain technology-neutral unless a clear rationale dictates otherwise, ensuring consistency with the approach generally adopted by sector regulators.
- Director criminal liability is disproportionate to directors' actual control over the threat environment and sits uncomfortably alongside recent government decisions to reduce personal director liability in other regulatory regimes, including around climate related disclosures and health and safety requirements.
- The proposed 30MW generation threshold may still capture assets whose loss would not materially affect system security and would benefit from further refinement.
- Compliance costs will be material for the electricity sector. Cost recovery is only available to price-quality regulated lines companies. Generators and retailers operating in competitive markets will carry costs directly and recover them through consumer prices, at a time when affordability pressures for consumers are already a concern.
- The growing digitalisation of the consumer-facing electricity supply chain introduces vulnerabilities that cannot be managed by critical infrastructure entities alone and are not addressed in the discussion paper.
- Ministerial direction powers are appropriate for genuine national security threats, but the safeguards must be commensurate with the breadth of the proposed power, including statutory requirements for expert technical advice, cost recovery, and indemnity from contractual liability.

ERGANZ welcomes continued engagement with officials through the design of any legislation and supporting regulations, and would support the establishment of a cross-sector expert advisory group to guide detailed design.

Defining critical infrastructure

The principles-based approach

ERGANZ supports a risk and consequence-based approach to defining critical infrastructure. The tiered model (infrastructure, essential infrastructure, critical infrastructure, critical infrastructure of national significance) is conceptually sound and broadly aligns with how cyber risk is already assessed within the electricity sector.

However, the framework should distinguish more clearly between critical, important, and supporting assets within an entity's operations. The current drafting implies that all components of an entity providing essential services are in scope, which is not consistent with a risk-based approach. A retailer's customer-facing website, for example, is not in the same category of criticality as the systems that interface with the wholesale electricity market or the distribution network.

The 30 MW generation threshold

The proposed 30 MW threshold for generators connected to the wholesale electricity market is a reasonable starting point but applies uniformly across technology types in a way that does not reflect the relative criticality of different generation assets to system security.

Baseload generation (hydro and geothermal) provides firm capacity that is directly relevant to system security and frequency stability. The unplanned loss of a hydro or geothermal station above 30 MW would have immediate consequences for the national grid.

Variable generation (wind and solar) is, by its nature, intermittent. The system operator already manages variability in these assets as part of normal demand management. A wind farm that is not generating due to a cyber incident is, from a system security perspective, operationally similar to a wind farm that is not generating due to the absence of wind. Battery storage sits somewhere between these two categories, with firming capacity that is becoming increasingly material to system stability.

ERGANZ recommends that the 30 MW threshold be applied to baseload generation, with a higher individual site threshold, or an aggregate portfolio threshold, for variable generation. This would more accurately capture the assets whose cyber compromise would genuinely affect system security, while avoiding compliance costs on assets whose intermittency is already managed within the system.

We also recommend that further consideration of the wording of the relevant threshold is also required as generators don't technically connect to "the wholesale market", but rather they connect to electricity transmission or distribution networks and operate within the wholesale market. This is a matter an expert advisory group could help with.

The definition of components

The proposed definition of components (assets, information, networks, systems, suppliers, people, and processes) is very broad. The requirement to map all components and the dependencies between them would impose significant and ongoing costs without a corresponding uplift in cyber security.

We recommend that the definition be narrowed to components with a direct and demonstrable impact on the delivery of essential services. This would focus compliance effort on the systems that matter most and would align with the risk-based philosophy of the regime.

Cascade effects and interconnected entities

The discussion paper acknowledges that cyber incidents can cascade across sectors, and Figure 1 usefully illustrates the interdependencies between energy, water, communications, and other sectors. However, cascade effects cut both ways. If the regime inadvertently treats every entity connected to critical infrastructure as itself being within scope, the regime becomes unworkable.

The interdependencies with other sectors also reveal threshold alignment problems. A cyber incident affecting water supply to a region where significant generation is located could affect the electricity system in ways that are not reflected in the sector-specific thresholds. For example, if drinking water supply to the Waikato were compromised, this could directly affect generation capacity in that region. The discussion paper should be explicit that obligations attach to the

protection of the essential service in question, not to every entity that is digitally connected to a critical infrastructure entity.

Interaction with the Emergency Management Bill

The discussion paper indicates that the definition of essential services will align with that in the Emergency Management Bill. The Emergency Management Bill definition is intentionally broad and designed for a response-phase emergency management context. It is not well suited as a trigger for ongoing, threshold-based cyber security obligations.

ERGANZ recommends that the cyber security regime adopt a tailored definition of essential services, or supplement the Emergency Management Bill definition with limiting criteria, to provide the regulatory certainty that critical infrastructure entities need. We also recommend that a clear mapping of the interaction between the Emergency Management Bill and the cyber security regime be published before the legislation is finalised, to identify areas of overlap, duplication, and potential conflict.

Ministerial designation and exemption powers

ERGANZ supports the Minister having powers to designate or exempt critical infrastructure entities, subject to appropriate consultation and lead-in time. Designations should not be made at short notice. Where a designation is made, the affected entity should have a reasonable period within which to implement any new obligations.

Information sharing and collection (Measures 1 to 3)

Measure 1: Government collection of information

ERGANZ supports the intent of building a common operating picture of the critical infrastructure system. However, information collection powers should be constrained in three ways. First, the information collected should be limited to what is genuinely necessary for national risk management. Second, requests should avoid duplicating information already held elsewhere in government. Third, a report-once principle should apply across government so that entities do not have to report the same information to the Electricity Authority, the Commerce Commission, the NCSC, the critical infrastructure regulator, and any other agency.

The electricity sector already reports extensively. The Electricity Authority operates detailed information requirements through its EIEPs and market systems, the Commerce Commission receives information disclosures from regulated lines companies, and asset management plans are already in the public domain. The critical infrastructure regime should build on these existing flows rather than creating a parallel reporting stream.

Measure 2: Voluntary information exchange

ERGANZ supports the establishment of a cross-sector voluntary information exchange. The electricity sector already participates in the Cyber Security Sector Information Exchange and finds it

valuable. A well-designed cross-sector mechanism could usefully sit alongside the existing sector-specific exchanges rather than replacing them.

The design of the exchange matters. A larger, more diverse group may lessen information sharing, particularly where members are unsure who might see sensitive disclosures. Consideration should be given to a tiered model, with a smaller group for critical infrastructure of national significance and a larger group for broader cross-sector engagement, as has been done in Australia.

We also support allowing participation by smaller entities that do not meet the critical infrastructure thresholds. Many of the digital service providers to the electricity sector are smaller entities, and their inclusion in an information exchange would strengthen the overall resilience of the sector.

Measure 3: Mandatory sharing between critical infrastructure entities

ERGANZ has significant concerns about mandatory sharing of commercially sensitive information between critical infrastructure entities. The scope of information that could be required, including system architecture, dependency mapping, restoration timelines, and operational capabilities, has the potential to provide competitors with operationally sensitive intelligence.

In the electricity sector, generators and retailers compete directly with each other in a market context. Mandatory sharing of restoration timelines or system architecture between competing gentailers raises legitimate competition concerns that are not addressed in the discussion paper.

We recommend that Measure 3 be either dropped in favour of supporting voluntary exchange, or narrowed substantially in scope. If retained, the information to be shared should be defined through a joint government-industry process rather than determined unilaterally by the regulator, and the protections against commercial misuse must be robust.

Protecting shared information

We support the proposed framework for protecting information shared with or collected by the government, including the proposed offences for government agencies that breach information protections. These protections are essential to maintaining industry trust in the regime.

The protections must be embedded in statute with clear consequences, and must not be diluted through subsequent regulation or administrative practice. Without robust and enduring protections, the quality of information shared will decline, undermining the outcomes the regime is intended to support.

Incident reporting (Measure 4)

Timelines

ERGANZ supports the 24-hour early warning and 72-hour follow-up report structure in principle. The timelines themselves are workable and broadly align with international practice, including the EU NIS2 Directive.

What matters is the content expected within those timelines. Within 24 hours, most entities will have only a preliminary understanding of the incident. The content required at the 24-hour mark should therefore be limited to a defined set of minimum fields: the nature of the incident, the systems affected, the estimated impact on essential services, and initial containment actions taken. Additional information should be provided on a best-endeavours basis.

The 72-hour report should be reframed as a best-available report, with a commitment to iterative updates as further information becomes available. For sophisticated, multi-vector, or state-sponsored attacks, complete forensic understanding may take weeks or months. A rigid expectation of a definitive report within 72 hours risks producing inaccurate or misleading information that would undermine rather than support NCSC's situational awareness.

Definition of cyber incident and significant cyber incident

The definition of a significant cyber incident is tied to serious impact on the delivery of essential services. The scope of essential services therefore becomes very important. As set out in our comments on defining critical infrastructure, the Emergency Management Bill definition is too broad for this purpose, and a more precise definition is needed to provide regulatory certainty.

The definition of a cyber incident (without the significant qualifier) is particularly important because this drives the regular reporting obligation. Large digital entities experience security events and alerts continuously as part of normal network operations. The definition must clearly exclude routine security activity that does not result in operational impact or compromise, otherwise the regular reporting obligation will generate volumes of information that provide little benefit.
Frequency of regular reporting

ERGANZ recommends quarterly reporting of impacting cyber incidents (as distinct from significant incidents requiring 24-hour notification). Quarterly reporting strikes an appropriate balance between providing useful situational awareness and avoiding an administrative burden that does not contribute to security outcomes.

We do not support regular reporting of all cyber events below the threshold of operational impact or compromise. Reporting at that level would just generate noise.

Limited use obligation

The limited use obligation is one of the most important features of the reporting framework. The discussion paper rightly acknowledges that the Government's priority on receiving an incident report should be swift remediation and recovery, not immediate compliance action. This intent must be given clear statutory force.

Without robust statutory protection, entities will involve legal counsel early in the reporting process to manage the risk that disclosures will be used against them in later proceedings. This will slow reporting, reduce candour, and undermine the partnership model the Government is seeking to build.

We recommend that the limited use obligation apply to voluntary incident reporting to the NCSC as well as to mandatory reporting, consistent with the Australian approach.

Risk management programme (Measure 5)

Alignment rather than compliance

ERGANZ supports the requirement for critical infrastructure entities to maintain a cyber risk management programme. It is already industry best practice to do so, and many of our members align with internationally recognised frameworks such as ISO/IEC 27001 and the NIST Cybersecurity Framework.

The discussion paper lacks clarity on whether it intends compliance with or alignment to a recognised framework. The distinction is material. Strict compliance obligations can produce a checklist mentality rather than a genuine risk-based response, and cyber security frameworks cannot always keep pace with a highly dynamic threat environment.

ERGANZ recommends that the legislation require alignment to a recognised framework, with the flexibility for entities to adapt and evolve their approach as the threat landscape changes. This is consistent with the discussion paper's own principle that legislation should not become rapidly outdated.

Framework selection

We support the discussion paper's proposal that the Government should not prescribe a single acceptable framework. Entities should be permitted to select the framework most appropriate to their sector and operational context, with a requirement to justify the selection.

We note that internationally recognised frameworks are strongly preferable to a New Zealand-specific framework. Building and maintaining a domestic framework would add cost and complexity without a corresponding security benefit, and would disadvantage New Zealand entities that operate internationally or use global vendors.

Process requirement, not substantive judgment

It should be explicit that the risk management programme obligation is a process requirement. A regulator should not be able to substitute its judgement for that of a critical infrastructure entity on which assets are critical, which risks are material, or how much risk treatment is enough. Entities are best placed to make these assessments about their own operations.

This is particularly important for the so far as reasonably practicable threshold for risk treatment. We support this formulation because it provides appropriate flexibility, and we recommend against any alternative language that would imply an absolute or risk-free standard.

Ministerial specification of additional measures

The power for the responsible Minister to specify additional risk management measures, or to require specific actions to manage particular risks, requires clear guard rails. In particular:

- Such specifications should be made only on the advice of the NCSC or equivalent technical authority.
- There should be a threshold test of necessity and proportionality before such specifications can be made.
- There should be a statutory consultation requirement with affected entities.
- The use of the power should be transparent, with publication of the rationale (subject to national security withholdings).

Reporting compliance

The staged approach to compliance reporting, starting with director attestation, moving toward a short report, and potentially toward third-party audit over time, is broadly sensible. However, we share the concerns raised at consultation hui that third-party audit is unlikely to enhance cyber security and is more likely to benefit consulting firms than to improve outcomes.

If director attestation is required and director liability attaches, directors will in practice require some form of external assurance. An alternative to full third-party audit could be attestation by appropriately qualified persons within the entity, potentially supported by internal audit review. This would provide assurance without generating the cost and capacity pressures that external audit would create.

Third-party and supplier obligations

The requirement for third-party vendors with operational control over critical components to support critical infrastructure entities in meeting their risk management obligations is, in principle, sensible. Digital supply chain risk is material in the electricity sector, where SCADA systems, energy management systems, market systems, and smart metering platforms are provided by a relatively small number of specialised, often multinational, vendors.

In practice, enforcing New Zealand-specific cyber security requirements on multinational vendors is difficult. Many of these vendors operate on standardised global product offerings and have limited commercial incentive to tailor their security posture to New Zealand requirements. Placing the full burden of managing vendor behaviour on the critical infrastructure entity, through contractual mechanisms alone, is likely to produce uneven outcomes.

ERGANZ recommends that the regime provide legislative backing that gives critical infrastructure entities genuine leverage over their vendors. This could include:

- Direct obligations on suppliers with operational control over critical components, backed by penalties, where those suppliers meet a threshold of criticality in their own right.
- A statutory right to terminate supply arrangements where a vendor cannot or will not meet the requirements, without liability for breach of contract.
- Clear recognition that entities are not liable for vendor non-compliance where they have taken reasonable steps to secure vendor cooperation via introduction of safe harbour

provisions that would apply in these instances, similar to under relevant health and safety legislation.

Clarification on the boundary between supplier and critical infrastructure entity

The discussion paper does not clearly address the relationship between supplier obligations and critical infrastructure entity obligations. Several scenarios require clarification:

- Where an entity is itself a critical infrastructure entity and also supplies critical components to another critical infrastructure entity, does it face additional obligations as a supplier beyond those that apply as a critical infrastructure entity?
- Where a supplier to a critical infrastructure entity does not itself meet critical infrastructure thresholds, is that supplier brought into the regime by virtue of the relationship, and on what terms?
- What obligations, if any, attach to suppliers that are outside the electricity sector (for example, cloud service providers, telecommunications providers, or IT managed service providers)?

These questions matter because smaller suppliers may respond to ambiguity by declining to service critical infrastructure customers. That would be a perverse outcome and would reduce rather than enhance the resilience of the system.

Consumer-facing digital devices

It is outside the discussion paper's scope to address the growing cyber risk associated with the consumer-facing digital electricity supply chain. As the electricity system becomes more distributed and digital, a significant and increasing volume of internet-connected devices are entering New Zealand homes: smart meters, home batteries, solar inverters, electric vehicle chargers, home energy management systems, and smart appliances that respond to pricing signals.

These devices are typically procured by consumers through retail channels, installed by independent contractors, and connected to home networks with variable levels of security. They create potential attack surfaces that can affect grid stability in aggregate, even if individual devices are not themselves critical. A coordinated attack on consumer-level devices, even at relatively low penetration, could create material grid instability.

Critical infrastructure entities have limited ability to manage this risk unilaterally. Retailers have no direct control over the security posture of devices their customers purchase from third parties. Distribution businesses have limited visibility of connected devices behind the meter.

ERGANZ recommends that the Government consider, as part of the broader cyber security strategy, minimum security standards for internet-connected consumer electricity equipment sold or installed in New Zealand. This could mirror approaches taken in the United Kingdom and European Union under consumer product cyber security legislation. This is outside the scope of the critical infrastructure regime itself but could be addressed alongside it.

Ministerial direction power (Measure 6)

ERGANZ accepts that a last-resort ministerial direction power is warranted in genuine national security situations. The electricity system is too important to national security and public safety for the Government to be left without options in an extreme situation.

That said, the breadth of the power as drafted (to do, or refrain from doing, anything necessary) is significant, and the safeguards around its use must be commensurate.

Safeguards

We support the proposed natural justice protections (consultation, appeal to the Minister, statutory review, indemnity against legal liability, and limits on acquisition of property). These should be augmented in several ways:

- Directions should be issued only on the basis of formal technical advice from the NCSC or equivalent authority. This is particularly important for directions that would affect electricity system operations, where the technical consequences of a direction may not be apparent to non-specialists.
- Directions affecting electricity system operations should also require advice from the system operator, as directions issued without that input could have consequences for grid stability.
- Directions should be of defined duration, with clear review mechanisms, and should not be capable of indefinite extension without fresh justification.
- Post-incident publication of the rationale for invoking the power is appropriate and should be mandatory, subject only to legitimate national security withholdings.

Cost recovery and compensation

The discussion paper states that there is no ability to seek damages or financial compensation for reasonable costs incurred in complying with a direction. This is a significant concern, particularly where the direction requires removal or replacement of existing technology.

Where an entity has made a capital investment in technology that was appropriate and unrestricted at the time of procurement, and a subsequent government direction requires its removal for national security reasons, the entity may be required to absorb very significant costs. Long-life assets such as battery storage, solar equipment, and grid-scale control systems involve capital commitments made on multi-decade investment horizons.

The Australian experience with the restriction and removal of certain telecommunications vendors from critical infrastructure networks demonstrates that government directions on national security grounds can impose substantial costs on affected entities. ERGANZ recommends that the regime include a mechanism for cost sharing or compensation where a direction requires removal of technology and the entity acted in good faith at the time of procurement.

Restricted vendor awareness

Entities procuring technology make decisions based on the information available at the time. Where the Government has concerns about particular vendors or technologies, entities need some form of early signal, even if less formal than a published list.

The discussion paper does not address how entities are expected to become aware of emerging vendor or technology risks in advance of a formal direction. This creates a risk that entities incur significant costs due to a lag in information sharing, with those costs falling entirely on the entity.

ERGANZ recommends that the Government work with industry to develop practical mechanisms for early awareness of emerging vendor and technology risks. This might include confidential briefings to critical infrastructure entities through established information exchange channels.
Contractual indemnity

The proposed indemnity against legal liability should extend to liability arising from breach of contract where compliance with a direction requires the entity to breach an existing contractual arrangement. Without this, entities may face competing financial pressures (the cost of compliance on one hand, the cost of contractual breach on the other) with no recourse.

Compliance, enforcement, and director liability

Director liability

The discussion paper proposes criminal penalties of up to $500,000 for directors for critical breaches, which include failure to meet minimum cyber security requirements. ERGANZ has concerns about this proposal.

The cyber threat environment includes state-sponsored actors with resources and sophistication that no commercial entity can fully match. The discussion paper itself acknowledges that state-sponsored actors have much greater ability and incentive to invest in exploiting a single vulnerability than any target could invest to reduce all of its vulnerabilities. It is inappropriate to recognise this asymmetry while simultaneously proposing personal criminal liability for directors whose organisations fall victim to such actors.

The proposal is also out of step with the Government's recent direction on director liability in other regulatory regimes. Recent reforms under the Credit Contracts and Consumer Finance Act, the climate-related disclosures regime, and the Health and Safety at Work Act have softened or removed forms of director liability, with the stated aim of reducing compliance-heavy burdens and avoiding overly risk-averse governance. The Law Commission is currently reviewing directors' duties and liabilities more broadly. Introducing a new form of criminal director liability for cyber security obligations would cut across that direction of reform.

The proposal is likely to produce several perverse outcomes:

- It will reduce the appetite of qualified directors to serve on boards of critical infrastructure entities, or require significantly higher remuneration to offset personal risk, at a time when these sectors already face governance talent shortages.

- It will push directors into operational detail rather than governance oversight. Good governance requires boards to maintain high-level oversight of business risks across all domains, not to immerse themselves in the technical detail of a single risk area.
- It will drive defensive governance behaviours and insistence on external audit assurance. This is the very outcome the discussion paper acknowledges would add cost without adding security.
- It will incentivise risk-averse decision-making at precisely the moment when the electricity sector's digital transformation and energy transition require bold investment.

ERGANZ recommends that:

- Criminal liability for directors be removed from the regime.
- Directors should be subject to a due diligence obligation analogous to that under section 44 of the Health and Safety at Work Act 2015. A director who can demonstrate that they exercised due diligence, including implementing a risk management programme, resourcing cyber security appropriately, and actively governing cyber risk at board level, should be protected from personal liability.
- Criminal penalties, if retained at all, should be reserved for demonstrated negligence or deliberate malfeasance, not for outcomes that were beyond the director's reasonable control.

Penalty proportionality

The proposed penalty structure for entities (the greater of a flat amount or a percentage of annual turnover) creates a significant disparity across entities of different sizes. For large electricity sector entities, 1 to 2 percent of annual turnover would result in penalties that are one or more orders of magnitude greater than the flat-rate amounts. Identical conduct by entities of different sizes would attract dramatically different penalties.

The discussion paper also lacks a clear definition of annual turnover. For an integrated gentailer, turnover can be calculated in a number of different ways and may vary significantly depending on the methodology applied.

We recommend that the definition of annual turnover be clarified, and that the relationship between flat-rate and turnover-based penalties be reconsidered to avoid disproportionate outcomes for larger entities.

Definition of minimum cyber security requirements

Critical breach includes failure to meet minimum cyber security requirements. Until the minimum requirements are defined with sufficient precision for entities to understand their obligations and assess compliance, it is premature to attach the most severe penalties in the regime to a failure to meet them.

Staged approach to compliance

We support the proposed one-year grace period between requirements coming into force and enforcement action being considered. Given the scale of the capability uplift required, a longer transition period may be appropriate for smaller entities or for more complex obligations.

Double jeopardy

The proposal that where a breach is punishable under multiple regulatory regimes, the more stringent penalty applies unless otherwise mutually agreed, is sensible in principle. However, the practical operation of this needs further thought, particularly given the number of regulators with potentially overlapping jurisdiction in the electricity sector.

Interaction with existing electricity sector regulation

The electricity sector is one of the most heavily regulated sectors in the New Zealand economy. The Electricity Authority regulates market conduct, system operations, retail competition, consumer protection, and increasingly the digital interactions between market participants. The Commerce Commission regulates Transpower and electricity distribution businesses through price-quality regulation under Part 4 of the Commerce Act. The Authority has specific powers in relation to operational resilience and has an active work programme that includes significant digital work.

The discussion paper acknowledges that the regime is not intended to replace or duplicate sector-specific regulation, and that where sector-based requirements meet the minimum requirements, the critical infrastructure regulator could issue a determination to that effect. In practice, this requires close and continuing coordination between the critical infrastructure regulator, the Electricity Authority, and the Commerce Commission. The discussion paper is light on how that coordination will operate.

We recommend that the legislation include explicit provisions for:

- Formal information-sharing arrangements between the critical infrastructure regulator and the Electricity Authority and Commerce Commission, with clear rules on confidentiality and onward disclosure.
- A single-regulator rule for entities where the Electricity Authority or Commerce Commission is already regulating the matter, with the critical infrastructure regulator taking a monitoring rather than primary role.
- A clear principle that where the Electricity Authority, in particular, has active regulatory processes underway, those processes should have precedence and should inform any subsequent action by the critical infrastructure regulator.
- An explicit recognition that the electricity sector's existing reporting obligations to the Electricity Authority and Commerce Commission provide a significant proportion of the information that the critical infrastructure regulator will require.

A significant volume of recent Electricity Authority work focuses on the granular digital communications between market participants and between participants and the Authority itself (the EIEP schedules, as-run generation, retail switching, and market information flows). These communications are increasingly real-time and machine-to-machine, and already carry cyber security obligations through the Electricity Industry Participation Code. The critical infrastructure

regime should recognise and build on this existing framework rather than layering parallel obligations.

Cost implications

Compounding costs across the electricity value chain

The proposed regime captures entities across the full electricity value chain: generation, transmission (Transpower), distribution (lines companies), and retail (in so far as retail systems interface with critical components). Costs incurred at each layer will ultimately be recovered through prices paid by electricity consumers.

This creates a tension with the discussion paper's stated design principle that cyber security should be enhanced at least cost to businesses, consumers, and government. ERGANZ recommends that the Government give explicit consideration to the cumulative consumer price impact of the proposed obligations before finalising the regime.

Cost recovery for competitive market participants

The discussion paper notes that entities subject to price-quality regulation may be able to recover compliance costs through additional revenue. This provides a potential recovery pathway for Transpower and for lines companies.

The same mechanism does not exist for generators and retailers operating in competitive markets. Those entities will carry compliance costs directly and will recover them through wholesale and retail prices. In an environment of already elevated inflation and ongoing affordability concerns, compliance costs imposed on the competitive segments of the electricity sector will translate directly into higher prices for consumers.
Scale of potential costs

While it is difficult to quantify compliance costs with precision at this stage, the experience of entities subject to similar regimes overseas provides some indication. The updated Australian regulatory impact analysis estimated average regulatory costs of approximately A$9 million per entity to transition to the full Security of Critical Infrastructure Act risk management programme framework, with ongoing annual compliance costs averaging A$4.1 million per entity for critical telecommunications assets.

Electricity sector costs in New Zealand would not be of an identical scale, but would be material. Costs would be incurred for:

- Administrative reporting and compliance infrastructure.
- Uplift of existing risk management programmes to align with prescribed standards.
- Retrofitting security controls into legacy operational technology, particularly SCADA systems where the discussion paper itself notes that approximately 35 percent of SCADA assets are at or nearing end of life.
- Supply chain assurance activities, including vendor due diligence and contract renegotiation.

- Personnel costs, including recruitment of specialist cyber security staff in a tight labour market.

ERGANZ members would welcome the opportunity to provide more precise cost estimates once the detail of the regime is clearer. Any cost-benefit analysis supporting final Cabinet decisions should explicitly account for consumer price impacts, not only business compliance costs.

Conclusion

ERGANZ supports the Government's objective of lifting the cyber security posture of New Zealand's critical infrastructure system. The electricity sector is already investing materially in cyber security, participates in voluntary information sharing, and takes the protection of essential services seriously. However, the regime as proposed requires further refinement before it can deliver proportionate benefits.

ERGANZ welcomes the opportunity to engage further with officials as the detailed design of the regime is developed. We would support the establishment of a cross-sector expert advisory group to guide the next stages, and would contribute actively to any electricity-sector-specific design process.

ERGANZ would like to thank DPMC for considering our submission.

If there are any outstanding questions or a need for further comments, please let me know.

Yours sincerely,

Kenny Clark
Policy Consultant