April 2026

National Security and Resilience Group
Department of the Prime Minister and Cabinet
Parliament Buildings
Wellington

Email: criticalinfrastructure@dpmc.govt.nz

Tēnā koutou

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

Scope of submission and summary

The Government's 2026-2030 Cyber Security Strategy and the Department of the Prime Minister and Cabinet's (DPMC) consultation document on Enhancing the cyber security of New Zealand's critical infrastructure system both frame stronger protection of critical infrastructure as a priority for national resilience and economic security.

The IoD supports this priority and the need for stronger cyber governance across New Zealand, including minimum cyber risk management standards for critical infrastructure entities.

New Zealand is facing a more serious threat environment, and a largely voluntary approach is no longer enough for critical systems and services that people and businesses depend on every day.

Our submission is focused on the role that directors and boards play within this critical system, and what it takes to support strong, effective governance for organisations responsible for critical infrastructure. We want to see a regime that will improve board oversight, strengthen organisational resilience, and work in practice for those governing critical infrastructure.

About the Institute of Directors

The IoD has over 10,500 members, is New Zealand's pre-eminent organisation for directors and is at the heart of the governance community.

We believe in the power of governance to create a strong, fair and sustainable future for New Zealand. Our role is to drive excellence and high standards in governance.

We support and equip our members who lead a range of organisations from listed companies, large private organisations, state and public sector entities, small and medium enterprises, not-for-profit organisations and charities.

We also supported ongoing professional governance development and recognise this through the Chartered Member pathway.

The central issue for the IoD is whether the proposed settings will improve compliance and resilience in practice. In our view, policy should be directed at the real barriers organisations and boards are dealing with, rather than relying on evidence-poor mechanisms such as personal criminal liability for directors.

Boards should be held to a strong standard of oversight, but the regime should not be designed around a standard of prevention that no critical infrastructure entity can realistically meet. We consider taking into account that the regime is new and complex, where new ways of attacking systems and technology are continuously emerging and evolving fast, where expectations are broad, open to judgement, and likely to change as the regime beds in. While the consultation document refers to a proportionate approach, the liability settings do not yet reflect one.

This concern sits alongside the Law Commission's current review of directors' duties and liabilities, which is considering the principles that should guide a more consistent and principled approach across legislation.

We appreciate that the proposed regime cannot wait for the Law Commission's recommendations. However, in the meantime, we consider that further duties should not be added to directors lightly, or without a clear case for why they are needed, how they fit with existing duties, and why they are the right lever to lift performance. The design choices in this regime may also carry weight beyond cyber. Once one liability model is set in a prominent regime, it can start to shape expectations elsewhere. That is another reason to ensure the settings are principled and proportionate.

In our view, the better path is to identify the real barriers to achieving the regime's outcomes, which include dealing with legacy systems, being locked into existing supplier dependencies, long replacement cycles, constrained capital, competing priorities (including dealing with other regulatory regimes), lack of capability and minimum training standards (at management and board level), limited assurance provider capacity and uneven levels of cyber maturity across entities, and then develop a regime that addresses those problems.

Summary of recommendations

The IoD recommends that:

- the primary compliance duty sit with the entity
- penalties for core obligations sit primarily with the entity and be set at a level that is proportionate and comparable with peer jurisdictions
- the board's role be framed clearly as one of oversight and assurance, with management responsible for implementation
- the regime recognise that directors already hold duties under the Companies Act and equivalent legislation, and avoid duplicating duties that already exist
- minimum cyber risk management requirements be supported by clear guidance, realistic implementation pathways and a credible approach to assurance

- personal criminal liability for directors not be included in this regime and, if it is retained, be confined to conduct that is clearly personal and plainly wrongful, such as knowing falsehoods, deliberate obstruction, or intentional non-compliance

- any attestation model sit with the entity and management, supported by assurance, recognising that the availability of qualified assurance providers is limited

- the regime recognise the reality of third-party and supplier dependence and avoid exposing directors for failures in environments they do not control

- materially equivalent obligations under other regimes be recognised clearly, with clear lead-regulator arrangements where more than one regime applies

- the regime be implemented through a staged compliance model, supported by practical guidance and a regulator capable of lifting standards across the system

- the implementation model include a focus on lifting capability across the system, including management capability, board capability and assurance provider capability, and recognise the importance of independent directors in challenging, influencing and supporting capability uplift

- the regime make clear that entities and boards are to be judged on how they identify, prioritise and manage material cyber risks over time, rather than on an assumption that every cyber incident can be prevented

- liability settings in this regime be justified by the particular features of critical infrastructure and not treated as a default model for later regimes.

The role of the board

We consider boards across New Zealand need to pay much closer attention to cyber security. Boards need to recognise that cyber security is a governance issue, not just an IT issue. It affects service continuity, organisational trust, investment decisions and response when something goes wrong. The IoD's 2025 Director Sentiment Survey found that only 55 percent of boards receive comprehensive reporting on cyber risk or data breaches, and that has barely shifted in three years.

DPMC's discussion document says directors would be responsible for ensuring compliance with the minimum cyber requirements. Those requirements are broad. They would require the organisation to identify critical systems and components, identify the cyber risks that matter most to them, and put in place a programme to manage those risks over time.

This work sits with management and the board's role is to govern it. It is the board's role to ask whether the framework is sound, whether management ownership is clear, whether reporting is good enough, whether issues are being escalated, and whether the organisation has a credible basis for assurance. Boards do not identify every system themselves, assess every technical risk themselves, or run the programme day to day.

The legislation should reflect the difference between management's role and the board's role more clearly. While we support high standards of governance and holding directors to account for oversight, we think that the directors' duties under the Companies Act, and equivalent legislation, adequately do this. We also acknowledge that the Law Commission is currently reviewing directors' duties under the Companies Act, and other legislation, and consider it is not appropriate to impose further duties on directors, particularly when they have not been thought through on a principled basis.

It should also be taken into account that good governance involves collective decision making. Cyber governance in practice is carried out through collective challenge, approval and oversight, while management is responsible for carrying those decisions into effect. A duty framed as "ensuring compliance" risks blurring that distinction. If that language is retained, the law should make clear that directors are being held to account for governance oversight, not for personally carrying out or guaranteeing management's implementation of the cyber programme.

The minimum cyber risk management duty

The IoD supports the idea of minimum standards. If New Zealand is going to have a stronger cyber security regime for critical infrastructure, there does need to be a baseline duty requiring entities to identify their most important systems, understand their key cyber risks, and put in place a programme to manage them.

This is the core obligation in the proposed regime. It will do much more work than the reporting requirements. It will shape what management has to build, what boards are asked to oversee, what investment may be needed over time, and how regulators will later assess whether the organisation has responded properly.

The difficulty is that this is not a checklist exercise. Frameworks such as NIST and ISO help organisations assess maturity, prioritise risk and guide investment. They do not provide a simple pass or fail answer. Organisations make judgements about where their most critical risks sit, what needs to be dealt with first, and what level of uplift is realistic over time.

Entities will also be starting from very different positions. Some will already have mature systems and strong controls. Others will be dealing with older infrastructure, supplier dependence, limited internal capability, long upgrade programmes and constrained capital. The same duty will therefore land very differently across the system.

The concepts in the proposal - critical components, material cyber risks and what is reasonably practicable - may sound well understood, but they still leave a great deal to judgement. In practice, organisations are unlikely to be able to prove compliance in any absolute sense. What they will be able to show is how they identified risk, what they prioritised, where they invested, what assurance they obtained, and how they made decisions over time. A proportionate regime should judge entities by the quality of that process and the credibility of the progress being made, rather than by an assumption that every cyber incident can be prevented.

For that reason, this duty needs to be framed and implemented carefully. It may be appropriate as an entity-level obligation, supported by clear guidance, realistic implementation pathways and a credible approach to assurance. It is a much weaker foundation for imposing personal liability on directors.

Personal liability for directors

The discussion document adopts a staged and proportionate compliance model. Lower-level breaches are dealt with through warnings, education, notices, monitoring and civil penalties. It also makes clear that entities and individuals would not be held responsible where the contravention was necessary to protect life or health or prevent serious property damage, was beyond their control and could not reasonably have been foreseen or prevented, was due to reasonable reliance on information supplied by another person, or was not known about and could not reasonably have been known about. Those protections are important and should be acknowledged.

Even with those protections, the proposal raises real concern. The examples of serious and critical breach show that director criminal liability would not be confined to deliberate wrongdoing. It would also extend to:

- negligent, reckless or knowing failure to review progress against minimum cyber security requirements,
- negligent, reckless or knowing failure to meet those requirements, and
- negligent, reckless or knowing provision of false or misleading information.

Directors could face criminal penalties of up to $100,000 for a serious breach and up to $500,000 for a critical breach.

Australia has taken a materially different approach in its critical infrastructure regime. Under the Security of Critical Infrastructure Act, core risk-management and incident-reporting obligations are enforced primarily through civil penalties on the responsible entity, with penalty levels that are much lower than those now proposed in New Zealand. That invites a legitimate question about why New Zealand's proposed director penalties are set at this level, and whether that setting is necessary to improve compliance and resilience in practice.

The difficulty is not the use of negligence in itself. Negligence can be an appropriate threshold where the underlying duty is clear and concrete. It is much harder to justify where the duty is broad, evaluative and still being worked through. Here, the proposed liability sits on top of concepts such as material cyber risk and what is reasonably practicable. Those are not bright-line tests. They require judgement about priorities, timing, investment and risk treatment in circumstances that may be changing quickly. Boards should be held to a strong standard of oversight, but not to a standard of prevention that no critical infrastructure entity can realistically meet. The relevant question is whether the entity identified its most material risks, prioritised the right work, invested sensibly, and made credible progress over time.

That difficulty is compounded by the fact that some of the most important cyber risks do not sit neatly inside the entity itself. The discussion document recognises that critical components may sit with suppliers and other third parties. For many critical infrastructure entities, key risks sit in cloud services, software vendors, managed service providers, data centres and other external dependencies. Boards do not control those environments directly. They oversee them through contracts, reporting, assurance and whatever leverage the market allows. Accountability should follow control and it should not be on directors to prove they don't have control.

A board may require reporting, approve funding, rely on management and expert advice, and oversee a credible programme of work, but still face the argument later that more should have been done. The proposed defences help at the margins, but they do not remove the central problem. They would still need to be argued after the event, often in circumstances where a regulator or court is looking back with more information than the board had at the time. In a regime of this kind, that creates a real risk of hindsight-based judgement.

In the IoD's view, the discussion document has not yet shown why personal criminal liability for directors is needed as part of this regime, or why it is likely to improve compliance more effectively than stronger entity-level duties backed by clear board oversight. The paper itself points to capability lift, implementation cost, limited audit capacity and phased implementation. Those are the practical barriers that need to be addressed if the regime is to work well. Current regulatory thinking points in the same direction. New Zealand's Ministry for Regulation says responsive regulation should start with cooperative measures and escalate according to willingness and ability to comply.

Liability settings also shape behaviour in more than one direction. They can sharpen focus, but they can also make boards more defensive, narrow legitimate risk-taking, and shift attention from improving resilience to managing personal exposure. The Law Commission has already recognised in its current review that some director duties are unclear and difficult to apply, and may discourage directors from taking legitimate business risks. Recent empirical work also suggests that liability settings affect who is willing to serve: a 2025 Management Science study found that stronger liability protection helped firms recruit higher-quality independent directors, while a 2021 Journal of Financial Economics study found that personal liability deterred board service and drove out expert directors. In a small market like New Zealand, with a limited director pool, those effects need to be taken into account. The burden is also not limited to conviction. The cost, reputational damage and personal strain of being drawn into criminal proceedings can be significant even where a prosecution does not ultimately succeed. The design choices in this regime may also matter beyond cyber. Once one liability model is set in a prominent regime, it can start to shape expectations in later regimes, whether or not the fit is right.

For those reasons, the IoD does not support personal criminal liability for directors in this regime. The better approach is to place the primary compliance duty on the entity, frame the board's role clearly around oversight and assurance, and support the regime with management certification, practical guidance and staged enforcement. If, despite that view, the Government decides to retain personal criminal liability, it should be confined to conduct that is clearly personal and plainly wrongful, such as knowing falsehoods, deliberate obstruction, or intentional non-compliance.

Attestation

The IoD does not support any form of attestation that would expose directors to personal liability for entity compliance with this regime.

New Zealand has already seen the risks of getting this wrong. In its review of the climate-related disclosures regime, MBIE concluded that the liability settings were encouraging overly risk-averse reporting, increasing legal and consultancy costs, and discouraging the inclusion of potentially useful information. Cabinet later agreed to remove deemed director liability for entity breaches, while retaining liability for misleading or deceptive conduct and false or misleading statements.

Where a regime is broad, forward-looking and heavily dependent on judgement, management input and evolving information, personal liability can distort behaviour and increase cost without improving the quality of reporting or decision-making. While the attestation process may be seen as a way of having to resort to third party assurance, it is unlikely to work in practice and directors will seek external assurance.

We suggest a better approach is to place the obligation on the entity and require management certification, supported by appropriate assurance. Boards can then be expected to oversee that process, test the basis for it, and hold management to account.

Overlap and duplication

This issue already arises in regulated sectors. In finance, a board may already be dealing with Reserve Bank requirements around cyber resilience, ICT risk and incident reporting, while also engaging with the Financial Markets Authority (FMA) on operational resilience and material incidents. In water, boards and governors are now operating in a system where Taumata Arowai and the Commerce Commission are looking at different parts of the same service. We have learnt that once more than one regulator is involved, the quality of the coordination matters considerably.

The concern is wider than duplicate reporting. Under the proposals, additional measures could be specified as part of the risk management programme and prescribed actions could be required to address particular risks. In a sector already subject to another regulator, that creates the possibility of different expectations about what work should be prioritised, what level of uplift is required, and what assurance a board should rely on.

Boards should not be left trying to reconcile competing regulatory signals about the same underlying resilience programme, or pushed into a sequence of investments driven by overlapping regulators rather than by a coherent view of risk.

The legislation should therefore do more than state a general intention to avoid duplication. It should clearly recognise materially equivalent obligations, identify the lead regulator where more than one regime applies, and make clear how conflicting expectations will be resolved in practice.

Reporting and ministerial direction

The IoD supports timely reporting of serious cyber incidents. Good information-sharing can reduce wider harm. But the reporting regime needs to work in the middle of a live event, when management is trying to contain the incident, keep services running and restore systems safely.

That means the reporting triggers need to be clear, the process needs to be workable, and overlap with other reporting channels needs to be kept to a minimum. If the threshold is uncertain, or if early engagement creates unnecessary legal risk, the regime is likely to produce delay, duplication and overly cautious communication at the very point where candour and speed matter most.

The same concern arises with the proposed ministerial direction power. The IoD accepts that government may need a reserve power for rare cases involving a serious national security threat. But if that power is to exist, the framework needs to be clearer about when it is used, who is in charge once it is used, and how it interacts with the board's existing duties and the entity's contractual obligations.

Implementation

These proposals will take time and money to put into effect. In many sectors, cyber uplift will involve legacy systems, supplier dependence, long replacement cycles, limited internal capability, and the need to sequence work alongside wider capital programmes and service obligations.

The discussion document itself recognises capability lift, cost, limited audit capacity and phased implementation. In our view, that is where the real compliance difficulties are likely to lie. Where those are the barriers, stronger personal liability for directors is unlikely to improve performance. Clear guidance, management accountability, access to external assurance, coordinated regulation and staged enforcement are more likely to do so.

A stronger regime will also depend on lifting capability across the system. That includes management capability, board capability, and the assurance market. Independent directors can play an important part in that uplift by bringing external perspective, challenging assumptions, and helping boards maintain focus on whether capability, investment and assurance are keeping pace with risk.

There is no formal minimum training threshold before a person can become a company director in New Zealand, so if government wants strong cyber governance it also needs to think about how that capability is built in practice. Some jurisdictions have gone further for at least some director roles, including mandatory training for first-time listed-company directors in Singapore and Malaysia, and proficiency requirements for independent directors in India.

Boards should be expected to take cyber resilience seriously and to show credible progress. But they should not be judged as though every organisation starts from the same level of maturity or can move at the same speed. The regime needs to recognise funding limits, legacy systems, supplier dependence, long replacement cycles, and the practical difficulty of changing critical infrastructure safely. A proportionate model should judge whether entities are identifying risk, prioritising the right work, and making credible progress over time.

Conclusion

The IoD supports a stronger cyber security regime for critical infrastructure.

Our main concern is with the way responsibility is allocated in the current proposal. The discussion document does not limit director liability to deliberate misconduct. It also proposes liability for negligent failure against broad minimum requirements that remain open to judgement. In our view, that is not a sound basis for personal liability in a new regime of this kind.

The better path is to place the main compliance duty on the entity, frame the board's role clearly around oversight and assurance, support the regime with management certification and practical guidance, and use staged enforcement to lift standards across the system.

That would give New Zealand a regime that is firm, workable and more likely to improve resilience where it matters.

IoD would welcome the opportunity to discuss any aspect of this submission further.

Institute of Directors New Zealand

Draft for member feedback