17 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

1. Thank you for the opportunity to make a submission on the consultation document Enhancing the cyber security of New Zealand's critical infrastructure system. New Zealand needs a stronger baseline for managing cyber risk across systems that matter for service continuity, economic resilience, and public confidence.
2. Our submission is focused on the governance issues that affect boards and directors. Cyber security is a governance issue because it affects continuity of service, organisational trust, investment decisions, incident response and resilience over time. The question for us is whether the proposed combination of requirements will improve resilience in practice. In our view, the proposed entity-level regime is directionally sound, but the current liability model is not workable in its current form.
3. Any resulting policy and legislative obligations should:

    a. **Place the primary compliance duty on the entity, with the board responsible for oversight, challenge, assurance, and lawful governance of compliance.** The proposed obligations depend heavily on management execution, operational judgement and sustained implementation over time. Boards govern that work, but they do not direct day-to-day delivery or control the operating environment in which that work sits.

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.

b. **Avoid personal criminal liability for directors and equivalent governors in a regime whose practical content remains uncertain and evaluative.** The proposal leaves unresolved questions about the nature of the obligation itself, including whether compliance turns on running a sound risk management process or on a later judgement that the substantive cyber work programme was insufficient. The duties are broad, the operating context is still evolving, and the proposal allows the content of the regime to expand over time. That is not a sound basis for criminal liability.

c. **Use implementation settings that strengthen resilience rather than drive defensive compliance.** The current attestation model is too blunt for a regime of this kind. It risks pushing boards towards defensive sign-off and more guarded reporting. It also risks shifting attention away from the practical barriers that will determine outcomes, including legacy constraints, external dependencies, capability gaps and implementation limits.

d. **Keep the regime proportionate in both cost and precedent.** The costs of compliance will extend beyond formal reporting and enforcement into the wider effort needed to build and sustain compliance. Those pressures will be felt across supply chains, including by smaller providers and SMEs. The regime should be designed around how entities identify, prioritise, and manage material cyber risk over time. It should not rest on an unattainable expectation that organisations can prevent every breach, and it should not create a liability template that later becomes the default model for other regimes without sector-specific justification.

4. Cyber attacks are crimes committed by offenders. In practice, this proposal risks placing criminal sanction on entities and directors who are themselves the target of that offending, even where the underlying issues turn on difficult judgement calls, evolving risks, management capability, supplier dependence, and the condition of systems over time. Existing governance duties already apply across the relevant legal forms. The immediate task is to establish a workable and proportionate entity-level regime that lifts resilience in practice.

Summary of submission points on proposed measures

Proposal	IoD position
Minimum cyber risk management requirements	The IoD supports a stronger baseline duty requiring critical infrastructure entities to identify critical components, identify material cyber risks, and maintain a programme to manage those risks over time. However, this is the core obligation in the regime and should sit with the entity. It should be assessed as an entity-level duty supported by clear guidance, realistic implementation pathways, and proportionate assurance.

Proposal	IoD position
Nature of the minimum requirements and accountability	Greater clarity is needed on the nature of the obligation. It remains unclear whether compliance turns on running a sound process for identifying and managing cyber risk, or on a later judgement that the substantive cyber work programme was insufficient. The level of uncertainty is important because the proposed duties are broad, evaluative, and dependent on management capability, supplier cooperation, system condition, and changing threat environment.
Governance settings: role of the board	The board's role should be framed clearly as one of oversight, challenge, assurance, and lawful governance of compliance. Management should remain responsible for implementation. Boards govern cyber risk, but they do not run the programme day to day, control every supplier or cloud environment, or directly manage every legacy system and upgrade pathway.
Enforcement: personal criminal liability for directors and equivalent governors	The IoD does not support personal criminal liability in this regime. The obligations are too uncertain, too evaluative, and too dependent on management systems, supplier performance, changing technologies, evolving attack methods, and regulatory judgement over time to justify criminal sanction. Existing governance duties already apply across the relevant legal forms, and are currently being reviewed by the Law Commission. The immediate priority for this regime should be a workable entity-level regime that lifts resilience in practice.
Enforcement: standard of liability	The regime should recognise that critical infrastructure entities cannot prevent every cyber incident. Boards and entities should be judged on how they identify, prioritise, and manage material cyber risks over time, rather than against an implicit expectation of perfect prevention. In practice, the trigger for liability risk is likely to be the fact of a serious incident, even where the organisation is itself the victim of criminal offending. That makes careful calibration of liability settings especially important.
Enforcement: if individual liability is retained	If Government nevertheless decides to retain some form of individual criminal liability, it should be confined to conduct that is clearly personal and clearly wrongful. That would include knowingly providing materially false or misleading information, deliberate obstruction, or intentional non-compliance with a requirement imposed personally on that director or governor.
Demonstrating compliance with minimum requirements	The IoD does not support the proposed attestation model in its current form. A formal declaration that minimum requirements have been met is too blunt in a regime built on evaluative judgements. It is likely to drive defensive assurance-seeking and legalistic sign-off rather than resilience uplift. The better model is entity-level compliance reporting supported by management certification and proportionate assurance.
Reporting of serious cyber incidents	The IoD supports timely reporting of serious cyber incidents. Reporting obligations and processes need to be workable in the middle of a live event, when management is trying to contain the incident, keep services running, restore systems safely, and make decisions with incomplete information. Clear triggers, coordinated reporting pathways, and practical expectations will be essential. The regime should also distinguish clearly between routine cyber events, cyber incidents, and significant cyber incidents, so that reporting obligations are tied to workable thresholds rather than ordinary operational activity.

Proposal	IoD position
Ministerial direction to manage a threat	The IoD accepts there may be a case for a reserve power for rare and serious national security threats. The proposal needs a clearer framework around when the power may be used, who is in charge once it is used, and how conflicts with other legal duties, service obligations, and operational constraints are to be managed.
Coordination across regulatory regimes	The regime should do more than express a general intention to avoid duplication. It should recognise materially equivalent obligations under other regimes, identify the lead regulator where more than one regime applies, establish single reporting pathways for the same incident, and provide a practical mechanism for resolving conflicting expectations.
Information-sharing and safe-sharing protections	There is a strong case for stronger protections for good-faith incident reporting and threat-intelligence sharing. Early reporting and timely sharing of threat information can reduce wider harm and improve resilience across the system. Settings that leave entities and directors concerned about additional legal or regulatory exposure may weaken those outcomes.
Suppliers and third-party dependencies	The regime needs to recognise the reality that many critical cyber risks sit with suppliers, contractors, cloud providers, software vendors, managed service providers, and other third parties. Boards govern those dependencies through contracts, reporting, and assurance, but they do not control those environments directly. Accountability settings should reflect where control actually sits. The impact will also flow through local supply chains, including to SMEs and smaller providers.
Implementation and capability lift	A stronger regime will depend on lifting capability across the system. That includes management capability, board capability, access to independent cyber expertise, and assurance provider capability. Government should focus early on practical guidance about what good looks like, what boards should expect from management reporting, what credible assurance looks like, and how equivalent obligations will be recognised.
Governance capability and access to independent cyber expertise	Government should consider whether boards of critical infrastructure entities should either include, or have direct access to, sufficient independent cyber expertise. Experienced independent directors and advisers can play an important role in challenging assumptions, bringing external perspective, and helping boards maintain focus on resilience over time. A cyber-focused board committee or advisory board may also be appropriate where that would strengthen oversight.
Implementation costs and proportionality	The regime needs to be proportionate in both design and cost. The costs will extend beyond formal compliance and enforcement into training, assurance, insurance, systems uplift, supplier management, governance capability, and the internal resources required to support reporting and certification. These pressures will be felt unevenly across sectors and supply chains, including by smaller providers and SMEs. A regime that pulls effort towards defensive compliance rather than practical resilience will increase cost without delivering better outcomes.

Proposal	IoD position
Broader regulatory precedent	Liability settings in this regime should be justified by the particular features of critical infrastructure and should not be treated as a default model for later regimes. Once a personal liability model is embedded in a prominent regulatory system, it can begin to shape expectations elsewhere and drive over-compliance beyond the context for which it was designed.

Governance and accountability

The role of the board

5. Boards across New Zealand need to pay much closer attention to cyber security. The IoD's 2025 Director Sentiment Survey found that only 55 percent of boards receive comprehensive reporting on cyber risk or data breaches.

6. Good board oversight starts with clear sight of the organisation's true cyber risk posture. Improvement often takes time, funding, sequencing, and sustained management attention, especially where entities operate across older and newer technology environments.

7. That perspective is central to our concern about personal criminal liability. Many directors already approach cyber with a strong sense of personal reputational risk and only limited grounding in the technical domain. In that environment, senior cyber leaders and other executives can already find it difficult to give free and frank advice when the position is uncomfortable or when remediation will take years rather than months. Personal criminal liability is unlikely to improve those conversations. A regime that leads boards to focus first on personal exposure is more likely to make reporting more guarded, more legalistic, and less useful. The same dynamic can add to the pressure on the managers and specialists responsible for cyber security in a market where capability is already thin.

Allocation of responsibility

8. The discussion document says directors of critical infrastructure entities, or equivalent governors, would be responsible for ensuring compliance with minimum requirements. Those requirements are broad. They require the organisation to identify critical systems and components, identify the cyber risks that matter most, and put in place a programme to manage those risks over time. This work sits with management. The board's role is to govern it by testing whether the framework is sound, ownership is clear, reporting is adequate, and capability and funding match the risk. Boards do not identify every system, assess every technical risk, or run the programme day to day. The proposal also does not yet make clear whether directors are being asked to stand behind the adequacy of the process that has been run, or the substantive sufficiency of the resulting cyber work programme.

Different governance settings across the system

9. Existing governance statutes already impose real duties on boards, directors and governors. Those duties differ across companies, Crown entities, statutory entities, local authority operators, and other forms of critical infrastructure provider. They were not designed as a uniform cyber enforcement code. Any new personal criminal liability in this regime therefore needs to be justified

with particular care, because it would overlay quite different accountability frameworks with one generic offence model.

10. This point becomes more acute once the range of covered entities is considered. A listed company board, a Crown entity board in health or transport, a State enterprise board, a port company board, and a local government body overseeing drinking water, wastewater, or stormwater infrastructure are not interchangeable. In local government especially, people may enter office because they have earned public confidence on broad representative grounds rather than through a skills-based board recruitment process. Yet some of those bodies oversee major infrastructure systems with substantial cyber exposure. It is easy to assume that all directors in this space are highly experienced commercial governors with strong technical support and substantial remuneration. Across the full system, that is not the reality. A workable regime needs to recognise who actually governs critical infrastructure in New Zealand and how capability is built in practice.

Collective decision-making and individual liability

11. Cyber governance is also collective. Boards govern through collective challenge, approval, and oversight. A personal criminal offence framed as ensuring compliance does not sit naturally with that model. Express dissent remains relevant, but it is not a complete answer to a continuing personal duty to ensure that the entity complied. The law should make clear that directors are being held to account for governance oversight, not for personally carrying out management functions or guaranteeing implementation.

The minimum cyber risk management requirements

A workable entity-level duty

12. The IoD supports minimum standards. New Zealand does need 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.

13. This is the core obligation in the proposed regime. It will shape what management must build, what boards must oversee, what investment may be needed over time, how assurance is approached, and how regulators later assess the organisation's response.

14. However, this is not a checklist exercise. Frameworks such as NIST and ISO help organisations identify risk, prioritise work, structure controls, and build maturity over time, but across a diverse system they do not naturally produce a simple pass or fail answer. Entities make judgements about priorities, sequencing and the pace of improvement.

Judgement and proof of compliance

15. Entities will begin from very different starting points and face very different implementation constraints. Mitigation may involve modest changes or significant long-term replacement work. The same legal duty will therefore land very differently across the system, especially where critical dependencies sit with external providers, including smaller domestic suppliers and SMEs.

16. The concepts at the heart of the proposal leave substantial room for judgement. They do not lend themselves to clear-cut verification, particularly as the threat and technology environment continues to evolve. 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.

17. This duty can work as an entity-level obligation, supported by clear guidance, realistic implementation pathways, and a credible approach to assurance. It provides a much weaker foundation for imposing personal criminal liability on directors while the regime is still taking shape, particularly while the proposal still leaves open a basic question about the nature of compliance itself: whether the law is requiring a credible process, a substantively sufficient cyber programme, or some uncertain combination of both.

Personal liability for directors and equivalent governors

18. The discussion document adopts a staged and proportionate compliance model, with lower-level breaches addressed through warnings, education, notices, monitoring, and civil penalties. It also proposes defences where the contravention was beyond a person's control, could not reasonably have been foreseen or prevented, resulted from reasonable reliance on information supplied by another person, or was not known and could not reasonably have been known.

Why the proposed liability model is unsuitable

19. The central difficulty is that the underlying duty remains broad and evaluative, and the examples of serious and critical breach are not confined to deliberate misconduct. They include 1) negligent, reckless, or knowing failure to review progress against minimum requirements within specified timeframes, 2) negligent, reckless, or knowing failure to meet the minimum requirements, and 3) negligent, reckless, or knowing provision of false or misleading information. In a regime of this kind, those defences operate after the event. They do not provide the ex ante clarity needed to justify personal criminal liability and they leave directors exposed to hindsight judgments made with more information than the board had at the time.

20. Criminal liability is easiest to justify where the underlying duty is clear, personal, and blameworthy, or where the conduct is plainly wrongful. The proposed liability would sit on top of concepts such as material cyber risk, reasonable person judgements, reasonably practicable treatment, framework selection, and evolving regulatory expectations. Those are not bright-line tests. They require judgement about priorities, timing, investment, and risk treatment in an environment that changes quickly. Boards should be held to a strong standard of oversight. They should not be treated as guarantors of an outcome that no critical infrastructure entity can realistically promise. Nor should the law move, in practical effect, towards punishing the victim of the crime when the organisation has itself been the target of cyber offending.

Strengthening cyber governance and resilience

21. Directors are already accountable under the governance law that applies to their entity for the matters that properly sit within the board's role. Existing criminal law may be able to address conduct that is truly personal and plainly wrongful, such as deception or obstruction, where the facts justify prosecution. The issue raised by this proposal is different. It would attach personal criminal liability to directors in relation to broad, evaluative cyber obligations that depend heavily on operational matters substantially outside directors' direct control. In the IoD's view, that is not the right way to strengthen governance or resilience.

22. That conclusion is reinforced by the practical barriers DPMC itself identifies. The paper points to capability lift, implementation cost, limited audit capacity, and phased implementation. Those are the issues that need to be addressed if the regime is to work in practice. New Zealand's Ministry for Regulation says responsive regulation should start with cooperative measures and escalate according to willingness and ability to comply.

Effects on directors and the director pool

23. Liability settings also shape behaviour. They can sharpen focus, but they can also make boards more defensive, push governance towards a compliance-only approach, narrow the space for responsible risk-taking, and shift attention from improving resilience to managing personal exposure. Good governance depends on boards being able to take reasonable, well-informed risks in pursuit of the organisation's purpose. A regime that leads boards to ask first what is safest for individual directors, rather than what will best strengthen the organisation over time, will not support better governance.

24. 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 deserve attention.

25. Experienced independent directors are part of the answer. They bring outside judgement, test management optimism, press for clearer reporting, and help boards stay with uncomfortable truths about cyber risk while the organisation lifts its position. In a complex critical infrastructure environment, a new director needs time to understand the organisation and its settings before they can contribute at full value. A liability model that narrows the pool of people willing to serve will slow the very uplift the regime seeks.

26. For company directors, the personal character of criminal exposure is especially relevant. Criminal liability itself cannot be indemnified or insured away under section 162 of the Companies Act, although limited support for certain defence costs is available in some circumstances. The consequences of criminal proceedings and conviction also extend well beyond the level of the fine. They can include reputational damage, effects on future appointments, practical constraints on

international travel, and heavy personal strain even where a prosecution does not ultimately succeed.

Limits of control and wider regulatory effects

27. Third-party dependence adds another layer. The proposal recognises that critical components may sit with suppliers or contractors and that contractual barriers may arise in the national security context. For many critical infrastructure entities, key risks sit in cloud services, software vendors, managed service providers, data centres, and other external dependencies. In the New Zealand context, those dependencies also run through local supply chains and smaller providers, including SMEs that may carry real cyber risk but have fewer resources to absorb compliance and uplift costs. Boards do not control those environments directly. They govern them through contracts, reporting, assurance, and whatever leverage the market allows. Accountability should follow control.

28. New Zealand has already seen the risks of getting liability settings wrong in a regime that is broad, forward-looking, and heavily dependent on judgement. In advice to Cabinet on amendments to the climate-related disclosures regime, MBIE said the liability settings were having a chilling effect on disclosures, encouraging a risk-averse approach to reporting, and increasing legal costs. Cabinet then agreed to remove deemed director liability for entity breaches. Where a regime depends on judgement, evolving information, and management processes, personal liability can drive defensive behaviour and higher compliance cost while doing little to strengthen governance or improve the quality of decision-making.

29. For those reasons, the IoD does not support personal criminal liability for directors and equivalent governors in this regime. If, despite that view, Government decides to retain some form of individual criminal liability, it should be confined to conduct that is clearly personal and plainly wrongful. That would include conduct such as knowingly providing materially false or misleading information, deliberate obstruction, or intentional non-compliance with a requirement or direction imposed personally on that director.

30. New Zealand should first establish the entity-level regime, build guidance and capability, and let the system settle in practice. That will provide a much clearer picture of what is working, where the real barriers lie, and what further changes are genuinely needed.

Attestation and demonstrating compliance

31. The IoD does not support the proposed attestation model in its current form. The proposal is a formal declaration that the minimum requirements have been met. In this regime, that is too blunt.

32. The declaration would amount to a sign-off on matters that depend heavily on judgement. Boards will seek assurance before standing behind a statement of that kind. Yet the proposal also says third-party audit is unlikely in the medium term because of cost and limited market capacity. It also remains unclear what, in substance, is being certified. Is the declaration intended to confirm that a credible process has been run, or that the resulting cyber work programme is substantively sufficient?

33. The likely result is a compliance exercise built around defensive assurance-seeking in a market that cannot yet support it. That will increase cost and shift scarce specialist capability towards sign-off rather than resilience. The same dynamic may encourage entities to default to paper compliance rather than genuine capability lift.

34. The better model is an entity-level compliance statement supported by management certification. That statement should explain the basis on which the entity considers the minimum requirements are being met, the framework being used, the assurance obtained, any material gaps or exceptions, and the remediation pathway. The board should oversee that process, test the basis for it, and hold management to account.

Overlap, duplication and regulatory coordination

35. Overlap and duplication already arise in regulated sectors and are likely to become more serious if this regime proceeds without clear equivalence and coordination settings. The concern goes beyond duplicate reporting to conflicting expectations about what entities must do and how they will be assessed where more than one regime applies.

36. Boards should not be left trying to reconcile competing regulatory expectations about the same underlying resilience programme, or pushed into investments driven by overlapping regulators rather than a coherent view of risk. In finance, boards may already be dealing with Reserve Bank expectations around cyber resilience, ICT risk, and incident management, while also engaging with the Financial Markets Authority on operational resilience and material incidents. In water, boards and governors are working in a system where Taumata Arowai and the Commerce Commission can each shape priorities.

37. The legislation should therefore do more than state a general intention to avoid duplication. It should provide a coherent coordination framework where more than one regime applies, including clear lead responsibility and a single reporting pathway. That would help contain unnecessary compliance cost and reduce the risk that boards are pulled towards regulatory process.

38. There is also a strong case for stronger protections for good-faith incident reporting and threat-intelligence sharing. Early reporting and timely sharing of threat information can reduce wider harm and improve resilience. The proposed limited-use protection does not provide a true safe harbour, because it may still leave entities and directors concerned that reporting will expose them to legal or regulatory risk. Government should consider whether stronger protection for good-faith reporting and information-sharing would do more to improve resilience than additional personal liability.

Reporting serious cyber incidents and ministerial direction

39. The IoD supports timely reporting of serious cyber incidents. Good information-sharing can reduce wider harm. The reporting regime still needs to work in the middle of a live event, when management is trying to respond under pressure and with incomplete information. Clear triggers and a workable process will be essential. Facts develop over time in a cyber incident. Early reporting may be necessary, but the regime should not assume that the significance, source, or likely impact of an incident will be fully understood at the outset.

40. The same concern arises with the proposed ministerial direction power. We accept that government may need a reserve power for rare cases involving a serious national security threat. The current proposal still leaves key questions. There may be circumstances where an entity is directed to take disruptive operational steps to contain a national security risk. That may be the right step. It can also create tension with service continuity and other legal or operational obligations. A clearer framework around when the power is used, who is in charge once it is used, and how conflicts with other legal duties and obligations are to be managed would improve the proposal.

Cost and proportionality

41. These proposals will carry real cost. Those costs will not sit only in formal compliance activity or enforcement exposure. They will also arise in training, management certification, assurance, advisory support, insurance, uplift of legacy systems, supplier due diligence, contract management, and the internal staff time required to support reporting and compliance across multiple regimes. In some environments, the most material costs will come from sequencing cyber upgrades across long-lived infrastructure while services continue and technology keeps changing.

42. Those pressures will not be confined to large entities. They are likely to flow through local supply chains, including to SMEs and smaller providers that support critical infrastructure entities and may face new assurance and contractual demands without the scale to absorb them. Cost alone is not a reason to avoid stronger cyber obligations, but it is a reason to design the regime carefully. Proportionality matters because a regime that drives expenditure towards compliance overhead will absorb resources that should improve resilience.

Implementation, capability and assurance

43. 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 regime will also need to work in a market where assurance capacity is limited.

44. A stronger regime will therefore depend on lifting capability across the system. That includes management capability, board capability, and assurance capacity. Government should focus early on practical guidance about what good looks like, what boards should expect from management reporting, what a credible assurance pathway looks like, and how equivalent obligations will be recognised. A heavy compliance posture without strong guidance is unlikely to produce better governance.

45. There is also a case for a more direct capability intervention. Government should consider whether boards of critical infrastructure entities should either include, or have direct access to, sufficient independent cyber expertise. Independent directors and advisers can bring informed challenge and perspective to board oversight.

46. New Zealand does not have formal minimum training thresholds before a person becomes a company director. If government wants stronger cyber governance, capability needs to be built deliberately through director development, clearer regulatory guidance, stronger management

capability, access to independent cyber advisers, and the cultivation of a deeper pool of capable directors willing to serve on critical infrastructure boards. A cyber-focused board committee or advisory board may also be appropriate where it would strengthen oversight and provide sustained attention to the organisation's risk profile.

47. Boards should be expected to take cyber resilience seriously and show credible progress. They should be judged on whether the entity is identifying risk, prioritising the right work, and making credible progress over time.

Conclusion

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

49. Our concern lies with the way responsibility is allocated in the current proposal. The discussion document proposes criminal liability for negligent or reckless failures against broad minimum requirements and review obligations in a regime that is new, staged, and still capability-constrained. In our view, directors and equivalent governors should not be subject to criminal liability in this regime. The proposal remains too unsettled and too dependent on matters outside directors' direct control to justify that step.

50. The immediate task is to establish a workable entity-level regime, supported by practical implementation settings and a staged approach to enforcement. That regime should be proportionate in both design and cost. Once the regime has been introduced and settled in practice, government will be in a much better position to assess how the system is operating and what further changes, if any, are genuinely needed. If personal liability is nevertheless retained, it should be confined to conduct that is clearly personal and clearly wrongful.

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

Ngā mihi nui,

Herman Visagie
General Manager, Governance Leadership Centre

Susan Cuthbert
Principal Advisor – Governance Leadership