NCC Group's response to the Consultation Paper: Proposed amendments to the Ministerial Directions Powers in Part 3 of the Security of Critical Infrastructure Act 2018

May 2026

Executive summary

NCC Group welcomes the opportunity to respond to the Department of Home Affairs' consultation. Drawing on our extensive experience advising and supporting a diverse range of Australian and global critical infrastructure (CI) entities, NCC Group seeks to provide practical, evidence-based considerations to inform the development and implementation of the proposed regime.

In brief, we recommend that the Government:

- **Embeds operational realities and sector-specific challenges into the design of Ministerial directions:** CI organisations typically manage risks associated with offshore managed service providers and high-risk vendors through their Critical Infrastructure Risk Management Program (CIRMP) obligations and contractual controls. The proposed powers introduce new layers of regulatory intervention that must be balanced against existing obligations, technical constraints and market dynamics.
- **Provides clear implementation timelines, proportionate milestones and practical guidance:** Flexibility is needed to accommodate multi-asset environments, supply chain dependencies and complex confidentiality considerations. Government should issue clear assurance templates and (board-suitable) compliance guidance, alongside considering targeted assistance to offset transition costs.
- **Takes steps to mitigate unintended systemic risks (e.g. price increases, supply constraints and service disruption):** These should include conducting robust competition and market impact assessments, sequencing transitions practically, establishing clear communication protocols, providing guidance, referenced architectures and shared contract clauses for new vendor agreements, and advising on supply chain alternatives (such as Five Eyes-acceptable options).
- **Embeds clear criteria and safeguards within the proposed delayed disclosure mechanism:** These should include thresholds for triggering national security or public safety threats, consideration of partial disclosure, and strict time limits (e.g. a hard limit of 90 days unless exceptional circumstances apply).
- **Coordinates post-implementation reviews:** Government should establish mechanisms for reviewing the effectiveness of directions and conditions (e.g. through the Cyber Incident Review Board).
- **Establishes proportionate penalty frameworks and procedural fairness:** Penalties must deter non-compliance without disproportionately affecting smaller CI operators. Appeals and review mechanisms should be available to ensure procedural fairness and defensibility.

NCC Group stands ready to support the Department and CI sector in developing a regime that is both effective and practical, ensuring that national security objectives are met without compromising operational resilience or market integrity.

About NCC Group

NCC Group's purpose is to create a more secure digital future. As experts in cyber security and risk management, our c.2,000 people worldwide are trusted by our customers to help protect their operations from cyber threats. Each year we dedicate thousands of days of internal research and development enabling us to stay at the forefront of cyber security and ensuring we secure the rapidly evolving and complex technological environment. As a global business operating in 12 countries, our regional Asia Pacific headquarters is based here in Sydney.

Nb. While NCC Group is not a critical infrastructure (CI) organisation, and therefore not subject to SOCI, we have insights to share drawn from our work supporting CI across a range of sectors. Therefore, in some cases, we have slightly reframed the consultation question to reflect this (i.e. replacing "your organisation" with "CI organisations").

Measure 1 – Amendments to the existing directions power in section 32

Q1. How closely does the scenario align with how similar risks are managed within CI organisations?

CI entities should, already, manage offshore managed service provider (MSP) dependencies as part of their Critical Infrastructure Risk Management Program (CIRMP) obligations. In our experience, CI organisations likely manage these risks through contractual controls and audits, rather than requiring direct government intervention.

Q2 Relative to maintaining the status quo, what non-regulatory or lighter-touch approaches (e.g. guidance, independent assurance, contractual undertakings) could reasonably achieve a similar outcome? Briefly rate feasibility and expected effectiveness.

We note the following considerations across the three alternatives proposed in the question:

- Independent assurance frameworks and security testing of pathways (e.g. ISO 27001[1], SOC 2 audits[2] and targeted red teaming, applied to the offshore MSP) would verify the existence and effectiveness of controls, and would be both moderately feasible and effective to implement.
- Contractual undertakings, such as requiring the MSP to limit privileged access to Australian-based personnel, would be feasible to draft, but enforcement is difficult

[1] https://www.iso.org/standard/27001
[2] https://www.aicpa-cima.com/topic/audit-assurance/audit-and-assurance-greater-than-soc-2

when the counterparty is a foreign state-linked enterprise with potentially limited Australian legal jurisdiction.
- Government-issued sector guidance (e.g. ASD Essential Eight applied to privileged access) would be low cost to implement. However, as outlined in the Department's consultation paper, uptake of guidance remains inconsistent without regulatory compulsion.

Q3 What internal steps and approvals would be needed to implement a direction of this kind (e.g., architectural changes, data/operational technology (OT) segregation, replacement of physical components, supplier re-papering, governance)?

The following steps would be required:

- A technical assessment, mapping the mentioned pathways held by the offshore supplier, and identifying dependencies on the MSP's tooling and people.
- An architecture redesign, including standing-up an Australian privileged access management (PAM) / identity access management (IAM) solution.
- Establishing a supplier contract addendum, repapering, potentially novating or terminating and onboarding a replacement provider, with appropriate security vetting in place.
- Seeking governance approvals and board approval for expenditure.
- Updating the CI entities' CIRMP to reflect the new architecture.

Q4 What is a realistic implementation timeline by milestone (e.g., design, procurement, migration, cut-over) while maintaining service continuity? Identify the top three schedule drivers (e.g., change windows, supplier lead times).

It would depend on the complexity of the multi asset CI entity. In setting expected implementation timelines, the Department should take account of dependencies (e.g. other CI entities, shared service providers) that could materially affect the ability to comply within the mandated timeframes.

Q5 What operational or risk-reduction benefits would you expect from implementing the direction (e.g., reduced likelihood of privileged compromise, improved mean time to detect/contain, fewer exception pathways)?

Benefits could include:

- Reduced systemic risk if it is servicing multiple CI assets.
- Reduced privileged access attack surface by removing offshore, foreign state-linked privileged access pathways, eliminating a possible vector for espionage or pre-positioning.
- Faster detection and response. It is also likely to be easier to perform digital forensics within the Australian legal jurisdiction.

Q6 What one-off activities would drive effort/cost (e.g., migration, tooling uplift, legal re-papering)? What ongoing activities would persist (e.g., monitoring, periodic assurance)?

Key one-off costs are likely to include the migration to a new PAM/IAM solution and the onboarding of a new supplier (e.g. contract termination clauses and establishing a new vendor agreement).

Entities are also likely to face costs (both one-off and ongoing) associated with an increase in their domestic workforce (including recruitment and training), particularly where a workforce was offshored.

Q7 Are there operational, contractual or technical impediments that would materially affect how CI entities could comply (e.g., vendor lock-in clauses, specialised OT equipment, data residency constraints)?

Yes. These include the following:

- Vendor lock-in, whether that's through customisation of a solution and/or contractual terms.
- Personnel vetting lead times for local hiring.
- A specialised solution may not be available locally. If the Department does move ahead with the measure, we strongly recommend exploring not only how it can support the growth of the domestic market, but also work with allied countries, such as the Five Eyes, to develop 'shared sovereign' solutions.

The Department should clarify whether compliance or staged risk reduction would be acceptable where full remediation is not immediately feasible due to contractual or technical constraints.

Q8 What board-level processes or approvals would you expect to trigger (e.g., risk acceptance thresholds, major capex approval, change of risk appetite)?

In addition to what is outlined under question 3 above, where relevant, if the Minister has given direction, the board may need to assess compliance with ASX disclosure which potentially conflicts with confidentiality directions**.** Section 674 of the Corporations Act 2001 mandates that listed entities immediately disclose "material" (price-sensitive) information to the market operator (e.g. ASX) if it is not generally available.

As proposed under measure 4 in the consultation, the Department should look to establish appropriate mechanisms to enable CI entities to be both in compliance of ASX Listing Rules and the proposed ministerial directions.

Q9 For corporate entities: Are there any legal or compliance interfaces under the Corporations Act that would need to be managed to comply with a direction (such as

continuous disclosure, related-party approvals, conflicts management, or director duty considerations)? What guidance from Government would assist board/company secretaries to document compliance?

Yes – see answer to question 8.

Q10 Would compliance have any material impacts on customers, prices, or service quality during transition? Are there cumulative burden issues when combined with other obligations (e.g., CIRMP, privacy, sectoral rules)?

A sector-wide restriction on a major vendor / hyperscaler could have a profound impact. It would likely lead to a concentration of demand on a small number of approved alternatives, which could, in turn, result in excessive pricing and supply constraints.

Depending on the CI entity, cumulative burden issues are likely to include concurrently managing CIRMP, privacy rules, sector-specific regulations, and now a potential vendor restriction – resulting increased capital and operational expenditure.

To reduce the overall burden on CI entities, the Department should ensure that sufficient and proportionate timelines for implementing a direction are given, while also considering whether government rebates and financial support for the necessary investments could be applied.

Q11. What success indicators (e.g., control maturity, reduction in privileged access exceptions, incident metrics) would show the direction achieved its objective? What support or guidance from Government would help (e.g., reference architectures, assurance templates)?

Success indicators might include:

- Systemic risk reduction across Australian CI systemic.
- CIRMP-tracked reduction in risk.
- Compensating for control effectiveness through independent, evidence-based assurance, including security testing and threat intelligence-led adversarial emulation and red teaming.

Government support should include:

- Referenced architectures (e.g. ASD publishing the most common approved implementation patterns, in line with ministerial direction).
- Shared contract clauses for new vendor agreements with embedded ongoing security assurance obligations, firmware verification, and Software Bill of Materials (SBOM) / Cryptographic Bill of Materials (CBOM) provisions.
- Lists of supply chain alternatives (e.g. Five Eye acceptable alternatives to help mitigate price gouging and supply constraints).

- Clear guidance on what evidence would reasonably be expected to demonstrate compliance with a direction at each milestone (e.g. design artefacts, contracts, control attestations, independent assurance).

More broadly, the Government should establish post-implementation review processes that would apply once a ministerial direction has been requested and completed, to inform future engagements (potentially where a service provider is providing the service to multiple Australian organisations).

Measure 2 – Conditions Power

Q3 What internal steps and approvals would be needed to implement governance-focused conditions (e.g., board/committee resolutions, constitution or shareholder agreement changes, access control changes, security vetting for defined roles, independent audit engagement)?

On the technical side, board platforms would need to be reviewed to ensure they are capable of implementing the conditions and to safeguard against the circumvention of controls (e.g. penetration testing). Appropriate and auditable logging and alerting would also need to be implement.

Government protocols would need to be updated, including conflict of interest frameworks, charter and clearance requirements for the Security Risk Committee and information control measures.

Board members will also need to be trained on their obligations and changes.

Q7 Are there operational, contractual or technical impediments that would materially affect how organisations could comply (e.g., investor rights clauses, listing rule obligations for committees, identity/access tooling limits)?

As outlined in the consultation document, contractual clauses could affect an organisation's ability to comply.

Most enterprise board portal platforms support document-level access controls, but may not provide the permission matrices required to implement a fully tiered CIRMP access model. Custom configuration, additional modules, or migration to an alternative platform may be required, carrying additional cost.

Q8 What board-level processes or approvals would you expect to trigger (e.g., committee restructuring, conflicts management protocols, risk appetite changes)?

The question identifies the key processes this measure would likely trigger. Regarding risk appetite changes, it's worth noting that the conditions would alter the governance risk profile, potentially imposing constraints on the board that the board has not chosen. A formal review

of the entity's risk appetite statement and risk register would be required to reflect the changed governance arrangements.

Q9 For corporate entities: Are there any legal or compliance interfaces under the Corporations Act and related frameworks that would need to be managed to comply with conditions (such as director duties, related-party considerations, changes to constitutions, or disclosure obligations)? What guidance from Government would assist board/company secretaries to document compliance?

Directors who comply with the conditions could potentially be exposed to claims that they have breached their duty to act in the entity's best interests (e.g. commercial freedom, loss of investment). In addition, it remains unclear how listed entities manage ASX announcements in such scenarios. Further guidance across both areas would be needed should the Government choose to pursue this measure.

Q10 Would compliance have any material impacts on customers, prices, service quality or investor relations during transition? Are there cumulative burden issues when combined with other obligations (e.g., existing FATA conditions, CIRMP, Protective Security Policy Framework (PSPF), sectoral rules)?

Compliance could have material impacts across a number of areas, including how the entity manages its investor relations, potentially negative ramifications for the board's profile and noted concerns about the entity's commercial freedom. In turn, this could impact future foreign investment opportunities for both the entity that is directly impacted and wider CI entities and supporting services, as concerns around government interference grow.

Q11 What success indicators (e.g., reduction in access to sensitive materials by observer roles, improved independence in security-sensitive decisions, audit outcomes) would show the conditions achieved their objective in your context? What support or guidance from Government would help (e.g., template conditions, model committee charters, sample access matrices, assurance templates)?

Success indicators could include:

- No unauthorised access to an entity's CIRMP and related artefacts, determined through an audit of the organisation's logging.
- The independence of the Security Risk Committee, with all members holding clearance.
- Enhanced information within an entity's CIRMP, enabling better-informed risk mitigation actions.

Government support and guidance might include:

- A model Security Risk Committee charter, particularly for listed companies.

- Jointly developed Home Affairs, Australian Securities & Investments Commission (ASIC) and ASX guidance on how listed entities should manage their continuous disclosure.
- Clear guidance on how conditions should be adapted over time where ownership risks change (e.g. divestment, governance restructuring, exit of foreign investors).
- Guidance and support for organisations managing scenarios where the imposed conditions materially affect investor confidence.
- Guidance on the transition arrangements that would be required to safely implement conditions affecting board composition or governance structures.

Measure 3 – Restrictions on the use of high-risk vendors, products or services

Q1 How would a vendor-specific restriction of this kind interact with CI organisations' current technology stack, procurement cycles, network/OT architecture, and operational processes? Are there key differences from the scenario that would affect implementation?

While we could not comment on the specific interactions, we would expect the stated compensating controls would help to mitigate the risks where immediate removal is not possible.

It is important to note that network switches / routers are core infrastructure embedded throughout enterprise and operational technology (OT) networks. Their replacement would involve physical hardware removal, network reconfiguration, interoperability testing and security testing – with potential impacts on industrial control systems that may have longer lifecycles and are therefore more costly to replace.

Q2. Relative to maintaining the status quo, what non-regulatory or lighter-touch approaches could reasonably achieve a similar outcome (e.g., strengthened sector guidance, an industry code with independent audit, Government procurement restrictions only, enhanced vendor due-diligence/assurance)?

Given lighter touch approaches were used in the scenario, and uptake remained consistent, use of the proposed power could be justified.

However, alternative approaches also include:

- Phased information sharing on technology undergoing centralised government reviews prior to restriction.
- Mandatory reporting of entities exposure to the same technology risks.
- Enhanced vendor due-diligence requirements, mandating CI operators to obtain independent firmware verification and SBOM from vendors before procurement.
- Phased or partial remediation (e.g. restricting management access but retaining equipment).

In addition, human source code review and binary analysis through disassembly is increasingly augmented by AI and has come a long way with tools like Ghidra. Government measures might therefore also include mandating independent verification, disassembly and analysis of firmware.

Q3 What internal steps and approvals would be required to comply (e.g., asset inventory and criticality mapping, replacement program planning, network redesign/segmentation, firmware validation, contract variations or re-tenders, outage/change windows, customer communications)?

Compliance with vendor restrictions would require a structured program with multiple workstreams:

- **Procurement**: This includes identifying alternative vendors, running tenders and sourcing compliant replacements, while actively managing supplier lead times and systemic supply-chain dependencies (noting that restrictions can create market-wide bottlenecks, as seen in recent component shortages). Any alternative solution must be assessed to ensure it meets functional and security requirements, particularly in OT environments where interoperability, safety and lifecycle constraints are acute. CI organisations should also plan for the possibility that a replacement technology could itself become restricted in future, supported by timely Government guidance, security testing and transition planning. In parallel, organisations may need to vary existing contracts with the restricted vendor or supplier, noting that termination of support or maintenance arrangements can trigger penalties and other commercial impacts.
- **Asset inventory and criticality mapping**: A replacement program should start with asset inventory – knowing exactly what the entity has, where it is, and how critical it is. While a part of SOCI, large CI operators can lack a fully current asset register. Generating one is, itself, a significant exercise.
- **Risk-based replacement**: Not all instances of the restricted equipment will present the same risk profile. Replacement should be prioritised based on risk (e.g. equipment related to or adjacent to CI and Systems of National Significance (SoNS) first), underpinned by a structured risk assessment.
- **Network redesign and segmentation**: After the risk-based assessment, for equipment that cannot be immediately replaced, compensating controls (e.g. network segmentation, enhanced logging, access control uplift) need to be implemented – requiring architectural design work, not just configuration changes.
- **Lab and User Acceptance Testing (UAT)**: Replacement equipment must be validated in a test environment before deployment in production, particularly in OT contexts where untested changes could lead to safety issues.
- **Change planning**: Network changes would require scheduled maintenance windows, often requiring coordination with customers (e.g. around any potential outages) – particularly in the example scenario.
- **Assurance**: Technical assurance in validating both risk and remediation effectiveness may also be needed.

- **Customer / stakeholder communications**: CI operators may have obligations to notify customers of planned outages. If the ministerial direction itself is confidential, that could create issues and justifications that are not factual.
- **Board approval**: CAPEX and risk acceptance decisions will need board-level approval. The board will also need to give consideration to a situation where a replacement technology ends up under a restriction at a later date.

Q5 What security or resilience benefits would you expect (e.g., reduction in privileged/remote access pathways, lower probability of systemic compromise, improved detectability/forensics, reduced attack surface across interdependent assets, reduced mean-time-to-detect anomalies due to standardised telemetry)?

While CI entities will be better placed to advise on this question, possible benefits include:

- The risk / exposure around the undocumented remote access pathway is removed.
- Reduced systemic attack surface, as the technology mentioned would likely be deployed across the sector.
- Improvement through replacement equipment from vetted vendors with transparent firmware and SBOM. As per the question, standardised telemetry could improve mean-time-to-detect anomalies.
- The deterrence effect: the existence of the power could incentivise vendors to cooperate with Australian Government security requirements (e.g. firmware verification, SBOMs) to avoid being designated as high-risk.

Q7 Are there operational, contractual, supply-chain or technical impediments that could materially affect the ability to comply (e.g., vendor lock-in, limited comparable technologies, third-party dependencies, integration with legacy OT)?

As outlined in the example scenario, challenges around vendor lock-in and integration with legacy OT could arise. In some cases, the OT systems have lifecycles of 20+ years, and could be specifically designed and certified to operate with the restricted vendors' equipment.

There may also be limited comparable technologies where there is little or no functional equivalent available. This can create a further risk that a replacement technology is subsequently designated as high risk or becomes subject to restrictions, resulting in repeated transition costs and additional capital expenditure. This risk could be reduced through earlier Government visibility of prospective restrictions, clearer forward guidance, and targeted support (including grants) to stimulate development of suitable alternatives aligned to CI and OT requirements.

Q8 What board-level processes or approvals would you expect to trigger (e.g., major capex approvals, risk appetite changes, write-down decisions, customer notification strategies)?

The examples outlined in the question would be triggered. A customer notification strategy will be particularly critical if the ministerial direction is wrapped in confidentiality.

Q9 For corporate entities: Are there any legal or compliance interfaces under the Corporations Act and related frameworks that would need to be managed to comply with a vendor-restriction direction— such as continuous disclosure, asset impairment disclosures, or directors' duty considerations in balancing transition risk and service continuity? What guidance from Government would assist your board/company secretary to document compliance?

Yes. Where a vendor-restriction direction is likely to have material financial or operational impacts (i.e. significant replacement costs), listed CI entities may need to manage continuous disclosure and shareholder communications obligations, potentially in tension with any confidentiality associated with the direction.

Directors and company secretaries would also need to ensure decision-making is appropriately documented having regard to directors' duties (including acting with due care and diligence and in the best interests of the company), particularly where compliance requires balancing transition risk, service continuity, safety (including in OT environments) and expenditure.

Government guidance that would assist includes clear criteria and worked examples for assessing when, and how, disclosure should occur in the presence of confidentiality requirements.

Q10 What are the likely market and competition implications (e.g., near-term vendor concentration, price effects, supply constraints, interoperability impacts) during transition? Would compliance have material impacts on customers, prices or service quality? Are there cumulative burden issues alongside other obligations (e.g., CIRMP, privacy, sectoral rules)?

A sector-wide restriction on a major vendor (e.g. a hyperscaler or widely deployed network/OT supplier) is likely to create near-term vendor concentration as demand shifts to a small number of approved alternatives. This can drive price increases, extend lead times, and create supply constraints (including for components), and may introduce interoperability and integration challenges where legacy environments were designed around the restricted technology. During transition, these factors can materially affect customers through higher pass-through costs, constrained service capacity, delayed projects, and increased outage/change risk where replacement requires intrusive engineering work.

Cumulative burden is also likely, as CI entities would need to deliver replacement programs alongside existing obligations (including CIRMP uplift, privacy and sectoral requirements), with impacts on both CAPEX and OPEX and competing demands for specialised engineering and assurance resources.

To support proportionate decision-making and reduce unintended market distortion, Government could publish a standard process for assessing competition and market impacts (including consultation with relevant regulators) and provide practical guidance on transition sequencing and confidentiality so that entities can manage customer communications and market disclosure appropriately.

Q11 What success indicators would demonstrate the direction achieved its objective in your context (e.g., % removal or remediation by milestone, reduction in high-risk remote access paths, incident/near-miss trends, independent verification results)? What support or guidance from Government would help (e.g., reference architectures, interoperability/segmentation patterns, minimum telemetry/assurance requirements, SBOM formats, model contract clauses)?

Success indicators might include:

- Systemic risk reduction across Australian CI systemic.
- CIRMP-tracked reduction in risk.
- Compensating for control effectiveness through independent, evidence-based assurance, including security testing and threat intelligence-led adversarial emulation and red teaming.

Government support should include:

- Referenced architectures (e.g. ASD publishing the most common approved implementation patterns, in line with ministerial direction).
- Shared contract clauses for new vendor agreements with embedded ongoing security assurance obligations, firmware verification, Software Bill of Materials (SBOM) / Cryptographic Bill of Materials (CBOM) provisions.
- Lists of supply chain alternatives (e.g. Five Eye-acceptable alternatives to help mitigate price gouging and supply constraints).
- Clear guidance on what evidence would reasonably be expected to demonstrate compliance with a direction at each milestone (e.g. design artefacts, contracts, control attestations, independent assurance).

The Government would also need to implement coordination mechanisms where multiple CI operators rely on shared vendors.

Measure 4 - Delay continuous disclosure requirement

Q1 Is a delayed disclosure power necessary in high-risk cyber incidents, and what types of disclosure obligations (under the Corporations Act or otherwise) should it cover?

Yes, a delayed disclosure power is necessary. Premature disclosure of an active, state-backed intrusion into identity infrastructure supporting multiple CI sectors could directly

accelerate systemic impact. It is important that the power has further qualifications around scope and design.

In addition to the Corporations Act and ASX Listing Rules mentioned in the consultation document, other relevant obligations could include the following (depending on the type of breach):

- Privacy Act notifiable data breach obligations.
- Mandatory incident notification requirements under the Australian Prudential Regulation Authority's (APRA) CPS 234 for financial entities.
- Australian Energy Market Operator (AEMO) reporting for energy operators.
- Australian Communications and Media Authority (ACMA) for telecommunications firms.
- Disclosure obligations built into contracts with customers and partners.

In our experience providing crisis simulations to Executives and Boards, many organisations find the reporting landscape complex to navigate and can lack a proper understanding of their current obligations across regulators.

Q3 Are there any non-legislative disclosure obligations (e.g., contractual requirements during capital raisings or major transactions) that could prevent or undermine a delayed Corporations Act disclosure?

Cyber insurance policies typically require prompt notification of incidents as a condition of coverage. It would help organisations to provide guidelines and examples of the types of adjacent companies that could be informed (e.g. Cyber insurance, incident response retainers) and how such companies should be informed / read into an incident (e.g. NDAs, legal privilege). Ambiguity could lead to poor decisions to engage the right support structures to contain and eradicate a threat actor in a timely manner.

Q4 Who should hold the power to delay disclosure (ASIC, the Minister for Home Affairs, or both)?

The power to delay disclosure should ultimately sit with the Minister for Home Affairs, with appropriate and mandatory consultation of both ASIC and other key agencies such as the Australian Signals Directorate.

ASIC has no intelligence access, no formal relationship with ASD or ASIO, and no statutory mandate to make national security judgments. The Minister for Home Affairs, on the other hand, is advised by all of government's intelligence inputs and would have the greatest understanding of a CI related systemic impact.

However, once the CI impact and national security implications are understood and confirmed as reaching the threshold to delay, mandatory consultation with ASIC will be necessary because ASIC understands market impact, as per the examples in this section

(e.g. ASX listing rules (cont. disclosure / 3.1)). Additionally, ASIC could be a facilitator of interaction with other disclosure programmes.

Q5 What criteria should govern when a delay can be issued?

Credible national security or public safety threat based on specific intelligence or technical advice (from ASIO, ASD, or equivalent) that public disclosure of the incident would create a material risk of harm to national security or public safety, not merely that disclosure would be inconvenient or commercially damaging. The Government should also consider whether criteria should include active wider / systemic remediation.

In addition, where feasible, partial disclosure should be considered as the preferred initial approach, enabling entities to fulfil notification obligations while mitigating the risk of premature market impact. Given the likelihood of information leaks when multiple parties are involved, and the rationale behind mandatory notification and continuous reporting for listed companies, it is important to recognise that extended delays in disclosure can increase the risk of leaks and market volatility. Partial disclosure may also be used to facilitate trading halts or pending regulatory announcements, supporting market integrity during sensitive incident response periods.

Q6 What safeguards, time limits, and oversight mechanisms are needed while still enabling effective risk management?

As outlined under questions 4 and 6, safeguards should include:

- Mandatory consultation with ASIC, ASD and ASIO before issuing a delay.
- Clear definitional thresholds that reporting would create a material risk of harm to national security or public safety.
- Consideration of whether partial disclosure would be preferred.

Clear guidance for entities will be essential, particularly given the existing lack of understanding around mandatory notification requirements (see question 1). The introduction of new powers is likely to increase complexity and create additional uncertainty. Targeted guidance for executives and boards on the operation and implications of any delay direction will be critical to ensure compliance and effective risk management.

In terms of time limits, the delay should only be as long as necessary to mitigate the wider systemic material risk. In practice, this should include a hard limit of 90 days unless there are exceptional circumstances – which would, in turn, require additional mandatory consultation with ASIC.

Q7 What operational or compliance impacts might arise during a delay?

Board directors could face heightened stress due to their statutory duties and personal legal exposure, often necessitating legal privilege advice – particularly in scenarios where share price may be affected or customer service level agreements (SLAs) are breached.

Prolonged delays in disclosure can increase the risk of insider trading and, as incidents persist, the likelihood of information leaks rises, potentially resulting in market speculation and short positions.

A delay direction may require the implementation of a trading halt at an appropriate juncture, with careful consideration given to the duration of such halts and the potential need for repeated actions. This underscores the importance of providing clear reasoning and, where necessary, partial disclosure to maintain market integrity and regulatory compliance.

Q8 What guidance, tools, or support would entities need to meet their obligations under this power, and how should the market be informed once a delay is lifted?

To ensure effective market integrity and compliance during delayed disclosure periods, we recommend the following measures:

- Establish a pre-approved trading halt mechanism, as referenced under Q7, to support timely and coordinated market interventions.
- Provide clear, authoritative instructions from the Minister regarding director duties, explicitly confirming that non-disclosure is legally required and offering directors protection from personal liability.
- Issue practical guidance on when and how entities may communicate with contractual partners, SLAs, third parties, customers, auditors and insurers during a delay.
- Provide clear guidance on what controls are needed to manage insider knowledge and prevent information leakage during a disclosure delay.
- Upon lifting the delay, implement coordinated disclosure procedures, including explanations from ASIC and the Minister for Home Affairs to the market, and mandate incident review by the Cyber Incident Review Board as proposed in the Cyber Security Strategy.

Q9 Are there relevant international practices that should inform the model, and what unintended consequences should be considered?

Relevant international practices that the Government should consider include: the U.S. Department of Justice's delay mechanism under the Securities and Exchange Commission's (SEC) cybersecurity rules[3]; and the UK's National Cyber Security Centre's (voluntary) practice of coordinating with listed companies on disclosure timing for significant cyber incidents.

[3] https://www.justice.gov/d9/2023-12/DOJ%20Cyber%20Incident%20Notification%20Delay%20Guidelines.pdf

Measure 5 – Increased civil penalty provisions

Q1 Does the proposed increase in the maximum civil penalty (from 250 to 2,000 penalty units) provide an effective deterrent to non-compliance with Ministerial directions under Part 3 of the SOCI Act? Why or why not? / Q2 What level of penalty would you consider proportionate to the seriousness of failing to comply with a direction issued to manage a material national security risk?

The proposed increase in the maximum civil penalty would strengthen the deterrent effect for non-compliance; however, for large CI operators or hyperscalers, even 2,000 penalty units (i.e. c. $660,000) is unlikely to be a significant deterrent.

That said, we understand that courts retain full discretion to set penalties, and the maximum is not necessarily the expected penalty in practice. As seen in other regulatory schemes, such as the Privacy Act, a turnover-based alternative may be appropriate. Indeed, the Government must also ensure penalties do not disproportionately affect smaller or less-resourced CI operators.

Q4 What guidance or support would assist CI organisations to understand and meet compliance expectations under an updated penalty framework?

Clear instructions from the Minister to directors are essential, explicitly outlining obligations and confirming whether failure to comply may result in personal liability.

Additionally, an appeals or review process should be available to entities subject to Ministerial directions or penalties, ensuring procedural fairness and providing a mechanism for challenging or reviewing decisions.

Q5 Do you foresee any unintended consequences of increasing the maximum penalty?

Higher penalties could influence directors' and officers' perceptions of risk, potentially making them more cautious or reluctant to accept roles within CI organisations.

The prospect of exposure to substantial penalties must also be considered in insurance and investment decisions, as it may affect the cost and availability of directors' and officers' liability cover and could influence investor confidence.