NATIONAL AUSTRALIA BANK SUBMISSION

Proposed Amendments to the Ministerial Directions Powers in Part 3 of the Security of Critical Infrastructure Act 2018

May 2026

National Australia Bank Limited ABN 12 004 044 937 AFSL and Australian Credit Licence 230686

Introduction

National Australia Bank (NAB) welcomes the opportunity to provide feedback on the Department of Home Affairs's Consultation Paper: "*Proposed amendments to the Ministerial Directions Powers in Part 3 of the Security of Critical Infrastructure Act 2018 (SOCI Act)*" (Consultation Paper).

Executive summary

As a major bank with critical infrastructure assets, NAB strongly supports the objectives of Part 3 of the SOCI Act, which empowers the Government to respond decisively and at pace to serious national security risks to critical infrastructure. This will become even more important with the growth of AI-enabled cyber threats, including the emergence of frontier AI models, which amplify the speed, scale, and sophistication of threats to critical infrastructure owners and operators.

NAB recognises the powers under Part 3 are intended to operate as exceptional, last-resort tools to be used where other regulatory, supervisory or cooperative measures cannot adequately mitigate a threat. Consistent with this intent, NAB believes that such powers should remain tightly constrained, applied only in extreme circumstances of material risk, and be subject to robust safeguards, coordination, and oversight.

NAB is broadly supportive of the intent of the five targeted measures. Overall, they appear aligned with feedback provided by the private sector (including NAB) in response to consultations on *Developing Horizon 2 of the 2023–2030 Australian Cyber Security Strategy* and the Independent Review of the SOCI Act, which called for clarity on the use of directions and appropriate guardrails on their exercise. In NAB's view, the reforms should:

- preserve the last-resort character of ministerial directions;
- maintain robust evidentiary thresholds for threat advice;
- minimise unnecessary operational disruption; and
- provide clear legal protections for entities acting in good faith under a direction.

As AI-enabled cyber threats increase the speed, scale and sophistication of threats, NAB also reinforces the importance of the continued operation of appropriate safe harbour frameworks that provide important protections and encourage entities to share timely and accurate information about cyber incidents. Full, frank and prompt disclosure by businesses that are being attacked, without fear of penalty or detrimental impacts, is critical to strengthening Australia's cyber resilience. The more intelligence that government, industry and the community can share about threat actors without regulatory implications, the better our collective response can be.

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

NAB supports the proposal to remove rigid preconditions (the need for an Adverse Security Assessment (ASA) and the "regulatory exhaustion" requirement) and replace them with more flexible requirements. These changes should help reduce delays in exercising the power and ensure the power can be more effectively used in time-critical risk scenarios. It will be important, however, to ensure the last-resort nature of the power is preserved (i.e. that the Minister should only use Part 3 directions after exhausting alternative remedies and good-faith negotiation with the affected entity). This recognises there are other means – e.g. technical guidance and targeted

supervisory communication – that could be used to effectively influence and apply pressure on suppliers with respect to expected security controls before escalating to a ministerial direction.

NAB recommends ensuring that tailored Australian Security Intelligence Organisation (ASIO) advice maintains a high evidentiary standard and comparative thresholds with respect to the security threat (replacing, but not weakening, the former ASA threshold). NAB expects ASIO's threat assessment would still need to be compelling for a direction to be made, and that the Minister would need to act reasonably and proportionately based on that advice, with the ultimate decision being subject to judicial review.

Recalibration of the "regulatory exhaustion" requirement recognises it may be unclear whether another regulator "could" act, and the Government should not be unnecessarily delayed by that uncertainty, as long as it acts reasonably. NAB supports this change, provided there is adequate coordination with other regulators wherever reasonably possible. In the banking sector, NAB would expect consultation and coordination with financial regulators (e.g. the Australian Prudential Regulatory Authority (APRA)) if the issue touched on prudential or market stability matters. NAB welcomes the expansion of consultation requirements to include relevant Commonwealth Ministers and agencies before a direction is issued. This will help ensure the Minister considers a broad range of factors beyond security threats when making the direction, including economic and social impacts.

Finally, NAB suggests clear legal protections would be required for entities acting in good faith under a direction to ensure they are not exposed to liability under other laws or contracts. The SOCI Act currently provides certain immunities for compliance with Government directions in emergencies (under Part 3A) and protections on disclosure of protected information. NAB encourages the Government to review whether analogous immunity provisions should be explicitly extended or clarified for actions under section 32 as amended. Reasonable implementation timelines for changing vendors will also need to be considered. For a large, regulated bank like NAB, this will involve detailed planning and design, disengagement from an existing vendor, procurement of a new vendor, implementation and testing and switchover of operations – a process that would likely take several months.

Measure 2 – Conditions Power

NAB recognises the value of a conditions-based approach to managing persistent risks in a proportionate way, as outlined in the Consultation Paper. This acknowledges there is currently a class or risk (e.g. those stemming from who controls or runs a critical infrastructure asset) that may not be readily solvable under the current power. NAB agrees this change could help address governance vulnerabilities in a more targeted and predictable manner, rather than repeated ad hoc directions for persistent governance-based risks. Importantly, the conditions power proposal builds in strict procedural safeguards, including a requirement for the Minister to consult with the entity and relevant agencies, consider less intrusive alternatives, and periodically review any conditions imposed to ensure they remain necessary.

NAB considers it is important to ensure any conditions imposed on reporting entities complement rather than conflict with other legal frameworks (e.g. the Corporations Act). NAB notes the proposal explicitly requires consideration of directors' duties and other regulatory regimes when imposing conditions.

NAB would welcome further guidance from the Government on how entities should manage any disclosure obligations that might arise from the conditions themselves. For example, if changes

remain over a long term, there may be challenges in keeping them confidential, especially if they require changes visible to shareholders, such as changes to board composition. The Government may wish to consider exempting an entity from disclosing the existence of a conditions direction, similar to the options being considered as part of Measure 4 on delaying continuous disclosure requirements.

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

NAB acknowledges Government action may be required to address a systemic supply chain vulnerability that cannot be mitigated entity-by-entity (e.g. if a particular foreign-manufactured technology was discovered to have vulnerabilities, e.g. concealed backdoors). NAB notes this power is conditioned on a high threshold – that the Minister must determine the vendor/product poses a material risk to national security and other measures cannot adequately mitigate the risk. In that context, NAB suggests any such direction be exercised as an emergency measure for high-risk scenarios and be implemented in a way to minimise operational disruption and costs. It should be considered an exceptional tool, used only where voluntary or sector-led measures prove insufficient (e.g. strengthened guidance, procurement controls, contractual levers, and security and assurance standards for SOCI technology vendors). This recognises that single vendors often provide a broad and tightly integrated suite of technologies, and a vendor-wide restriction could disrupt a wide range of services unless carefully managed.

NAB supports the inclusion of risk-based targeting, reasonable transition timeframes and phased implementation (where appropriate) to maintain operational continuity. This ensures the power could allow for orderly risk reduction (rather than immediate shutdowns). It also recognises that transition to a suitable alternative will involve several phases (e.g. scoping, design and validation; procurement and security review; integration and operational testing; staged deployment and migration; and decommissioning), which would likely take several months.

NAB also supports the requirement for the Minister to weigh economic and service reliability impacts and consult affected parties wherever practicable. NAB sees this as crucial, given we rely on a vast array of hardware, software and service providers, including global vendors. A direction requiring the exit of all services provided by a particular vendor would have significant budgetary implications, and raise operational, reputational and legal risks. NAB would welcome further clarity on legal protections where compliance with a direction requires early termination or modification of a vendor contract.

To ensure effective operation of this measure, NAB emphasises the importance of the following safeguards:

- Proportional use and genuine need: power only used for truly high-risk situations where there is compelling evidence a vendor or product is compromised, or could be exploited in a way that endangers national security at a systemic level.
- Reasonable transition periods: ensuring a realistic schedule for any mandated change, so the security outcomes can be achieved without causing outages or unintended security gaps during the transition.
- Legal clarity: given a vendor ban could mean entities need to break contracts or service level agreements with that vendor or customers, NAB suggests inclusion of an explicit clause that makes it clear compliance with a Part 3 vendor direction is a defence to any legal claim arising from ceasing to use a product or service.

Measure 4 – Delay continuous disclosure requirements

NAB supports creating a narrowly scoped mechanism to temporarily delay an entity's continuous disclosure obligations in exceptional cases where public disclosure of a cyber security incident would threaten national security or public safety. A new SOCI Act-based direction (Option 2) may provide greater legal certainty than using section 111AT of the Corporations Act (Option 1), as it would create a positive legal obligation not to disclose. This in turn would enliven an exemption from continuous disclosure under the ASX Listing Rules on the basis disclosure would be a breach of law.

By contrast, Option 1 creates greater legal risk for the affected entity as it requires entities to interpret and apply the legislation and make their own assessment as to whether disclosure should be delayed. If the entity reaches an incorrect view, it remains exposed to significant liability for disclosure failures, including potential class actions.

Other benefits of Option 2 over Option 1 include:

- Scope limitation: Option 2 is framed to apply specifically in the SOCI context. This focuses the power on circumstances most likely to have national security implications.
- Operational speed: Under Option 2, the Home Affairs Minister could issue a direction promptly (with appropriate consultation), which may be more operationally efficient than requiring ASIC to consider and grant a separate exemption decision.
- Clarity on the decision authority: Under Option 2, the decision to invoke the power rests with the Home Affairs Minister, who is best placed to assess national security risks. Whereas, Option 1 relies on the Australian Securities and Investment Commission (ASIC), presumably based on Government advice related to a national security assessment.

More generally, any mechanism to delay disclosure will depend on information remaining confidential and a reasonable person not expecting the information to be disclosed. This creates legal uncertainty where confidentiality is lost, or is perceived to be lost, including through media reporting, service disruption or customer impacts beyond an entity's control. In those circumstances, it may be unclear whether a disclosure delay direction or exemption continues to apply.

Regardless of the model adopted, strict safeguards and oversight should apply. Safeguards should include:

- A high threshold ("extraordinary national security or public safety risk"), which in practice would likely mean involvement of government systems or multiple critical infrastructure sectors, or evidence of state-sponsored intent to cause widespread harm.
- Strict time limits: NAB suggests a short initial period (e.g. 30 days) with any extension requiring affirmative and time-bound renewal based on updated information. Government could also consider a hard cap on the number of renewals, or total duration for the delay (e.g. 60 or 90 days in extreme cases).
- Allowance for partial disclosure: NAB expects there will be instances where not all details need to be suppressed (e.g. a company may be able to inform the market of the existence of the incident in general terms, but postpone disclosing how an attack happened, if it wouldn't jeopardise a coordinated response).

For the regime to work effectively, adjacent legal and regulatory issues should also be addressed, including:

- the interaction with the Notifiable Data Breaches scheme under the Privacy Act;
- the inability for a company to rely on cleansing notices under the Corporations Act while disclosure is delayed (for example, in connection with capital raisings, security issuances without a prospectus), which could impact a company's funding needs and capital management activities; and
- in relation to the ASX, coordination to avoid companies being placed in conflicting positions – including how any disclosure delay would operate alongside ASX's power to require disclosure to correct or prevent a false market – this is particularly relevant in cyber incidents where confidentiality could be lost through service outages, customer impacts or media reporting beyond an entity's control, or where heightened market speculation results in unexpected movements in an entity's share price.

While Option 2 is preferable in addressing these issues, we strongly recommend the introduction of a clear statutory immunity for any breach of law or contract that arises as a result of good faith compliance with the disclosure delay direction. This should expressly cover civil liability (including misleading or deceptive conduct), regulatory enforcement and contractual obligations, to ensure entities acting in the national interest are not exposed to residual legal risk.

The Government should also consider developing guidance to companies on managing market communications during a delay (e.g. what could be said in the interim period) and also on disclosure expectations once any delay is lifted. This would help preserve confidence and transparency (i.e. if such a delay were used, it could be disclosed after the incident was contained or resolved). In the interests of transparency, the Government could also consider reporting on the number of times it invoked the continuous disclosure delay power (e.g. annually).

Measure 5 – Increased civil penalty provisions

NAB acknowledges the position outlined in the Consultation Paper that the present penalty for failure to comply with a direction may be too low to be a credible deterrent. NAB does not object to a calibrated increase in penalties as a deterrent and to underscore the importance of compliance, given the potential risks to national security. NAB also recognises that courts retain discretion to impose appropriate penalties on a case-by-case basis, and that this change would apply prospectively with guidance provided to industry on compliance expectations. Aligning the penalty with the enforcement framework already operating in Part 2D of the Act (for telecommunications carriers) also promotes consistency.

Significantly higher penalties heighten the importance of ensuring entities fully understand their obligations. NAB views this measure as appropriate, provided the Part 3 powers continue to be used sparingly and fairly.

Conclusion

NAB appreciates the opportunity to contribute to this important consultation. We look forward to continuing our active engagement with the Government as it refines the SOCI directions framework to ensure it remains agile and fit for purpose in managing serious risks to national security.