Level 27, Tower 1
International Towers
100 Barangaroo Ave
Sydney NSW 2000

1 May 2026

Critical Infrastructure Security Policy Branch
Department of Home Affairs
PO Box 25
BELCONNEN ACT 2616

Submitted electronically.

CONSULTATION PAPER: PROPOSED CHANGES TO THE MINISTERIAL DIRECTIONS POWERS UNDER THE SECURITY OF CRITICAL INFRASTRUCTURE ACT 2018

Introduction

FinTech Australia welcomes the opportunity to provide a submission on the Department of Home Affairs' consultation paper on the proposed changes to the Ministerial Directions powers (**Directions power**) under the *Security of Critical Infrastructure Act 2018* (**consultation paper**).

As the peak industry body representing Australia's fintech sector, we support reforms that strengthen the Government's ability to respond to serious national security risks affecting critical infrastructure, particularly where the current framework may be too rigid or procedurally cumbersome to operate effectively in time-sensitive circumstances.

At the same time, the proposed reforms have implications extending beyond entities directly captured under the *Security of Critical Infrastructure Act 2018* (**SOCI Act**). Fintech firms are embedded across payments, data, identity, cloud and software layers that support critical infrastructure and may be affected indirectly through procurement decisions, contractual requirements, governance expectations and supply chain risk settings. For that reason, reform should be carefully calibrated.

This submission sets out FinTech Australia's position on each proposed measure and recommends a framework that is proportionate, clearly bounded and capable of practical implementation.

About FinTech Australia

FinTech Australia is the peak industry body representing the Australian financial technology sector, with a membership of more than 400 companies and startups nationwide. Our members span the full breadth of the fintech ecosystem, including payments, consumer and business lending, artificial intelligence, wealthtech, regtech, neobanking, open banking, digital assets, distributed ledger technologies, DeFi, and Web3. The fintech industry delivers a wide range of business-to-business and business-to-consumer financial products and services that support the smooth operation of the Australian economy.

Our vision is to position Australia as one of the world's leading markets for fintech innovation and investment. This submission has been compiled by FinTech Australia and its members in an effort to advance public debate and drive cultural, policy and regulatory change toward realising this vision, for the benefit of the Australian public.

Executive Summary

FinTech Australia supports reforms that strengthen the Government's ability to respond to material national security risks affecting critical infrastructure. The consultation identifies genuine limitations in the current operation of the Directions power framework, particularly where procedural requirements may constrain timely intervention in serious or time-sensitive circumstances.

At the same time, the proposed reforms are more than a technical adjustment to the existing framework. In FinTech Australia's view, the reforms point to a broader shift in how national security risk may be managed across critical infrastructure supply chains, governance structures and cyber incidents. Even if the formal legal perimeter remains unchanged, the practical reach of the regime is likely to extend well beyond entities directly captured under the SOCI Act. That matters for fintechs operating across payments, data, identity, cloud and software layers that support critical infrastructure.

In our view, the consultation paper has five practical implications for fintechs:

1. **Commercial risk for fintech suppliers -** Replacing the Adverse Security Assessment with an Australian Security Intelligence Organisation (ASIO) advice requirement, recalibrating the exhaustion test and keeping directions non-public collectively create a greater intervention power for the Government. For fintechs, however, the practical risk is commercial. Firms supplying regulated entities may face demands to change vendors, redesign access models or restructure governance at short notice, without visibility into the underlying direction driving the change.

2. **An expanded risk lens into ownership and governance -** The proposed conditions power extends beyond conventional cyber controls into questions of board composition, investor rights and information access. For fintechs, this means cap table and governance structures may increasingly matter to regulated customers, and investor rights that are standard in venture transactions may begin to be read as national security risk factors.

3. **A direct basis for sector-wide vendor intervention -** Many fintechs operate precisely in the layer most likely to be affected, including payments, fraud, identity, cloud, data and embedded software. Even where they are not themselves regulated under the SOCI Act, they may face effective de-selection by regulated customers responding to perceived concentration, ownership or privileged-access risks.

4. **Compliance obligations flowing through supply chains -** Directly regulated entities are likely to respond by imposing more demanding procurement, assurance and contractual requirements on their suppliers. For fintechs, that translates into longer sales cycles, more intensive due diligence, stronger contractual flow-downs and earlier investment in governance and assurance capability.

5. **Higher stakes around cyber incidents and disclosure -** For listed or disclosure-sensitive fintechs, particularly those in data or infrastructure-adjacent roles, the proposed disclosure powers signal a shift in which serious cyber events are treated as national security matters requiring government coordination, not solely as operational or disclosure obligations. For fintechs not directly captured under SOCI, the spillover effect is that larger counterparties may expect them to support confidential incident coordination and operate under tighter information-sharing constraints during an event.

Taken together, these measures point to a framework in which the boundary between a directly regulated infrastructure operator and a broader technology or service provider becomes less economically meaningful. From FinTech Australia's perspective, this gives rise to three central concerns.

1. **Barriers to entry**

   While the consultation paper acknowledges the need to consider competition impacts and disproportionate burdens, the overall direction of travel points toward higher compliance expectations, more intensive vendor diligence and greater risk conservatism among regulated entities. These dynamics tend in practice to favour larger incumbents over smaller challengers, even where the smaller firm is more innovative or offers a stronger product.

2. **Regulatory layering**

   These reforms sit alongside broader work on the SOCI Act, Critical Infrastructure Risk Management Program Rules, the Cyber Security Strategy and foreign investment settings. For fintechs already navigating payment service provider licensing, AML/CTF, scams, privacy and cyber obligations, the cumulative effect is likely to be significant. The burden will not arise solely through direct legal obligations. It will also materialise through overlapping expectations transmitted by banks, infrastructure providers and other regulated counterparties operating across multiple frameworks simultaneously.

3. **Uncertainty**

   A framework that relies on flexible drafting, non-public directions and case-by-case intervention grounded in intelligence-led risk assessments may make it difficult for firms to assess in advance what ownership structures, governance arrangements, vendors or operating practices will be regarded as acceptable. That uncertainty carries real economic costs. It can chill investment, extend procurement timelines and make enterprise customers more cautious about engaging with emerging fintech providers.

In that sense, this consultation points to a future in which the SOCI framework is less about a fixed list of captured entities and more about equipping Government with stronger tools to shape the broader ecosystem around critical infrastructure, an ecosystem in which fintechs are deeply embedded.

FinTech Australia's view is that the most effective reforms will be those that improve the operability of the existing framework while remaining clearly bounded, proportionate and capable of practical implementation. That requires clearer thresholds, stronger safeguards, better coordination with adjacent legal frameworks, and greater regard to the commercial and technical realities in which these powers are likely to operate in practice.

The final framework should strengthen national resilience without creating unnecessary barriers to entry, cumulative regulatory burden or avoidable uncertainty across the broader ecosystem.

FinTech Australia looks forward to continuing constructive engagement with Government as these reforms are developed to ensure the final framework is effective, proportionate and workable in practice.

Measure-Specific Considerations

1. Measure 1 - Amendments to Section 32

The proposed amendments would remove the requirement for the Minister to obtain an adverse security assessment before issuing a direction under section 32, and instead require the Minister to obtain and have regard to tailored ASIO advice. The consultation paper also proposes recalibrating the existing regulatory exhaustion test so that the Minister would consider whether

other regulatory mechanisms could address the relevant risk more effectively, while retaining negotiation, consultation and judicial review safeguards.

FinTech Australia supports the objective of improving the operability of section 32. The consultation paper identifies legitimate constraints in the current framework, particularly where procedural settings may impede timely intervention in circumstances involving serious and fast-moving national security risk. However, the following considerations should be kept in mind:

1.1. Commercial Risk and Compressed response timeframes for suppliers

For fintechs supplying regulated entities, the practical significance of this change extends beyond the legal settings of the power itself. A more agile and less visible intervention framework may compress response timeframes for counterparties and reduce the opportunity for suppliers to plan for or understand the basis of consequential changes to vendor, access or governance arrangements. That has implications for contractual management, service continuity and the ability of smaller providers to respond at pace.

1.2. Greater clarity on thresholds and advice

The proposed changes would also broaden ministerial discretion and reduce existing structural constraints. Concepts such as "*material risk*" and "*reasonably necessary*" define the scope of the power and should not be left entirely to case-by-case interpretation. Greater clarity around the factors informing those assessments would improve consistency, support more predictable administration, and reduce uncertainty for affected entities.

The framework would also benefit from greater clarity as to the role, nature and minimum content of that advice, particularly where it may inform directions with material operational, contractual or governance consequences.

Recommendation 1

FinTech Australia recommends that any expansion of the section 32 directions power be accompanied by clearer statutory and administrative guidance on the operative thresholds for intervention, including "material risk" and "reasonably necessary", together with greater clarity on the role and expected content of ASIO advice and the decision-making factors relevant to the exercise of the power. Guidance should also address the practical implications of non-public directions for affected entities and suppliers, including where consequential changes may need to be implemented within compressed timeframes.

2. Measure 2 - New Conditions Power

The proposed conditions power would enable the Minister to impose targeted conditions on reporting entities where ownership, control or governance arrangements create a material risk to national security that cannot be adequately mitigated through existing obligations or voluntary measures.

The consultation paper states that the power is intended to operate alongside, rather than duplicate, the *Foreign Acquisitions and Takeovers Act 1975* (FATA) regime. On that basis, FATA conditions would continue to address risks identified at the transaction stage, while the proposed SOCI power would address risks that arise, persist or intensify after an acquisition, or emerge outside the foreign investment approval process.

2.1. Governance and ownership implications

FinTech Australia recognises that governance settings may, in some circumstances, give rise to serious national security concerns that are not readily addressed through existing tools. At the same time, the breadth of the proposed power raises important design considerations. Board

composition, committee structures, investor rights, information access arrangements and internal decision-making processes are central to corporate governance and commercial practice. Intervention in these matters may have effects extending beyond the immediate security concern, including for capital formation, transaction structuring and the allocation of rights between investors, directors and management.

2.2 Implications for venture-backed fintechs

This is particularly significant in the fintech context, where venture investment structures and bespoke governance arrangements are common. A power that reaches into these settings may affect broader market expectations regarding acceptable ownership and control structures, with implications for investment certainty and capital formation.

For early-stage and growth-stage fintechs in particular, this signals a potential shift in market expectations around acceptable ownership and governance structures. Investor rights, observer seats, reserved matters and information access arrangements that are standard in venture transactions may increasingly be scrutinised as national security risk factors not only by regulators but by regulated customers conducting their own supply chain risk assessments.

2.3 Interaction with existing legal frameworks

The interface with directors' duties, broader corporate law obligations and the foreign investment regime requires more careful treatment. Where a direction bears upon board processes or governance settings, entities will require greater clarity as to how such directions are intended to operate alongside existing legal obligations and FATA-related processes. More explicit coordination would reduce the risk of duplication, inconsistent treatment and uncertainty as to the appropriate regulatory pathway.

Recommendation 2

FinTech Australia recommends that the proposed conditions power be confined to clearly defined circumstances involving material and demonstrable national security risk, and supported by robust review mechanisms, clearer limits on governance intervention, and more explicit alignment with the *Corporations Act* and the foreign investment regime. The framework should also provide practical guidance on the treatment of common venture governance arrangements.

3. Measure 3 - Vendor Risk Power

The proposed vendor-risk direction power would enable coordinated action where a vendor, or its products, equipment, services or technologies, presents a material risk to national security. The power could support directions to responsible entities individually or by class, including to cease using specified products, restrict future procurement, remove or remediate technologies, or implement compensating controls where immediate removal is not feasible.

3.1. Implications for fintech suppliers

For fintechs operating in payments, fraud, identity, cloud, data and embedded software layers, the risk is not limited to direct regulatory exposure. Even where a fintech is not itself captured under SOCI, it may face effective de-selection by regulated customers that conclude the vendor presents concentration, foreign ownership or privileged-access risk regardless of whether a formal direction has been issued.

3.2. Supply chain and procurement implications

These dynamics are also likely to extend beyond the immediate vendor relationship. The consultation paper's scenarios concerning offshore managed service providers, privileged access, subcontracting transparency, personnel assurance and vendor lock-in point to an

environment in which directly regulated entities will respond by imposing more demanding requirements on their own suppliers, including clearer subcontracting maps, stricter privileged-access controls, localised support arrangements, stronger assurance frameworks and independent audit obligations.

For fintechs operating within those supply chains, the practical effect is likely to be felt through procurement rather than direct regulation. It may mean longer sales cycles, more intensive due diligence, stronger contractual flow-downs and earlier investment in governance and assurance capability. In that sense, the SOCI framework may increasingly operate as a de facto market-shaping regime beyond its formal legal perimeter.

3.3. Implementation challenges

Vendor-related intervention is often difficult to implement in practice. Critical technologies are frequently embedded across multiple functions, integrated into broader operating environments, and delivered under global contractual arrangements that offer little or no scope for tailored renegotiation. As a result, substitutability may be limited and replacement may require redesign, migration, testing, customer remediation and re-certification. In some cases, no like-for-like alternative may be available within a commercially or operationally realistic timeframe.

3.4. Market impacts

These constraints should be reflected in the design of the power. The framework should provide for realistic transition periods, explicit recognition of contractual and technical limitations, and a clearer basis for determining when compensating measures are sufficient pending transition. In many cases, a staged transition, restricted deployment, enhanced monitoring or progressive isolation of higher-risk components may be more workable than immediate removal.

The proposed power may also have broader market effects. Vendor interventions of this kind may shape procurement behaviour across the sector. Where regulatory or quasi-regulatory expectations drive customers toward a narrower pool of perceived low-risk providers, the result may be reduced vendor diversity, increased concentration and diminished competitive pressure.

Recommendation 3

FinTech Australia recommends that the proposed vendor-risk power proceed only on the basis of a more developed implementation framework that recognises commercial and technical constraints, provides for reasonable transition periods, and requires explicit consideration of competition, concentration and market resilience impacts.

The framework should also address the cumulative compliance burden transmitted through supply chains, including through guidance to assist regulated entities in applying proportionate and consistent expectations to suppliers.

4. Measure 4 - Delayed Disclosure

The proposed measure would introduce a limited, time-bound mechanism to delay disclosure obligations in rare high-risk cyber incidents where public disclosure would threaten national security or public safety. The consultation paper proposes either relying on ASIC's existing exemption power under section 111AT of the *Corporations Act* or creating a new SOCI-based power under which the Minister could direct an entity not to publicly disclose the existence of the incident for a prescribed period.

4.1. Implications for fintechs

For listed or disclosure-sensitive fintechs, particularly those in data or infrastructure-adjacent roles, this signals a shift in which serious cyber events may increasingly be treated as national

security matters requiring government coordination, not solely as operational or market disclosure obligations. For fintechs not directly captured under the SOCI Act, the spillover effect may still be significant. Regulated counterparties may expect them to support confidential incident coordination and operate under tighter information-sharing constraints during an event. In practice, this may create de facto obligations outside any formal legal framework.

4.2. Interaction with existing disclosure obligations

Further, the proposed model intersects with a number of obligations that are already complex in practice, including continuous disclosure obligations under the *Corporations Act*, ASX Listing Rules, and privacy and data breach requirements. Contractual disclosure obligations may also arise in financing, transaction and customer settings. Any delayed disclosure mechanism will therefore need to provide a clear and reliable basis on which entities can assess the legal effect of a delay decision and its interaction with existing obligations.

This is particularly important for boards and management teams making time-critical decisions during a cyber incident. The applicable thresholds should be narrow, duration should be limited, and the framework should provide clear guidance on the legal consequences of delay across the relevant disclosure settings.

FinTech Australia considers that use of an existing mechanism, such as section 111AT of the *Corporations Act 2001* (Cth), may provide a more proportionate and administratively coherent pathway, provided it is supported by clear criteria, efficient processes and practical guidance. Any final model should proceed on the basis that delayed disclosure is exceptional, with defined time limits, active review, and clear expectations as to when ordinary disclosure obligations resume.

Recommendation 4

FinTech Australia recommends that any delayed disclosure mechanism be limited to exceptional circumstances and subject to tightly framed thresholds, defined time limits and active review. It should also be supported by clear guidance on how a delay decision interacts with continuous disclosure, ASX Listing Rules, privacy obligations and relevant contractual disclosure requirements. Where practicable, this should be achieved through an existing mechanism, such as section 111AT.

5. Measure 5 – Civil Penalties

The consultation paper proposes increasing the maximum civil penalty for non-compliance with a Ministerial direction under Part 3 from 250 to 2,000 penalty units. FinTech Australia recognises the rationale for ensuring that penalty settings reflect the seriousness of non-compliance with a Ministerial direction in the context of national security risk. If the Ministerial directions framework is to operate as a more active intervention tool, it is reasonable to consider whether the existing penalty level remains fit for purpose.

5.1. Clear and workable compliance obligations

At the same time, stronger penalties should operate within a framework where underlying obligations are clear, proportionate and capable of practical implementation.This is particularly important where compliance with a direction may involve operational change, third-party dependencies or phased implementation over time. In those circumstances, the effectiveness of a higher penalty setting will depend not only on deterrence, but also on whether entities have clear guidance as to what compliance requires in practice.

Recommendation 5

FinTech Australia recommends that any increase in civil penalties be accompanied by clear compliance expectations, practical implementation guidance and a continued emphasis on proportionate enforcement, so that stronger penalties operate within a framework that is precise, workable and fair in application.

Conclusion and next steps

FinTech Australia appreciates the opportunity to contribute to this consultation and looks forward to continued engagement with the Department of Home Affairs.

FinTech Australia supports the objective of ensuring the directions framework remains capable of responding effectively to serious national security risks affecting critical infrastructure. Against that background, the proposed reforms would broaden the practical reach of the regime beyond entities directly regulated under the SOCI Act. Taken together, they are likely to increase commercial risk for fintechs supplying regulated entities, expand scrutiny of ownership and governance arrangements, provide a stronger basis for vendor de-selection, reinforce the flow-through of compliance expectations across supply chains, and raise the stakes around cyber incidents, disclosure and enforcement.

For fintechs, that is likely to mean higher barriers to entry, greater regulatory layering and increased uncertainty as the practical perimeter of the regime expands beyond entities directly captured under the SOCI Act. In FinTech Australia's view, the framework should proceed on the basis of clear thresholds, proportionate safeguards, practical implementation pathways and strong coordination with existing legal and regulatory regimes.

FinTech Australia welcomes continued engagement as these reforms are developed. To arrange a meeting, please contact [redacted]

Yours sincerely,

[redacted]
FinTech Australia