Australian Government
Department of Home Affairs

Consultation on proposed amendments to the Ministerial Directions Powers in Part 3 of the *Security of Critical Infrastructure Act 2018*

Purpose of consultation

The Department of Home Affairs consulted on proposed amendments to the Ministerial Directions powers in Part 3 of the *Security of Critical Infrastructure Act 2018* (SOCI Act) to test the case for reform and the practical operation of the proposed powers. Consultation focused on whether the amendments would provide Government with effective, targeted and proportionate tools to respond to serious national security risks affecting critical infrastructure, while preserving appropriate safeguards for regulated entities.

The Department sought feedback on the proposed thresholds for using the powers, the role of consultation and security advice, interactions with existing regulatory frameworks, and the practical implications for affected entities if a direction, condition, vendor restriction or disclosure delay were issued. Consultation also tested implementation issues including operational feasibility, service continuity, transition timeframes, legal certainty, contractual impacts, cost drivers and guidance needs.

Feedback from consultation has informed the final policy design for the proposed Bill and will continue to inform implementation guidance, including around safeguards, consultation requirements, mandatory considerations, transition settings, legal certainty for good-faith compliance and practical guidance for industry and government.

Engagement overview

The Department used a combination of public consultation, written submissions, sector briefings and targeted follow-up engagement to test the proposed reforms with affected stakeholders and gather evidence on practical implementation issues. This engagement helped identify stakeholder views on the policy objective, proposed safeguards, interactions with existing regulatory frameworks, and the potential operational, legal and economic impacts of the reforms.

- Public consultation opened on 25 March 2026 and closed on 1 May 2026.
- The Department received 50 written submissions from critical infrastructure entities, technology and cybersecurity providers, business and governance bodies, financial services and market infrastructure stakeholders, energy, telecommunications, water, health, public sector bodies, civil society organisations and peak bodies.
- Written submissions provided the main evidence base for stakeholder views on the proposed measures, safeguards, legal interactions and implementation risks.

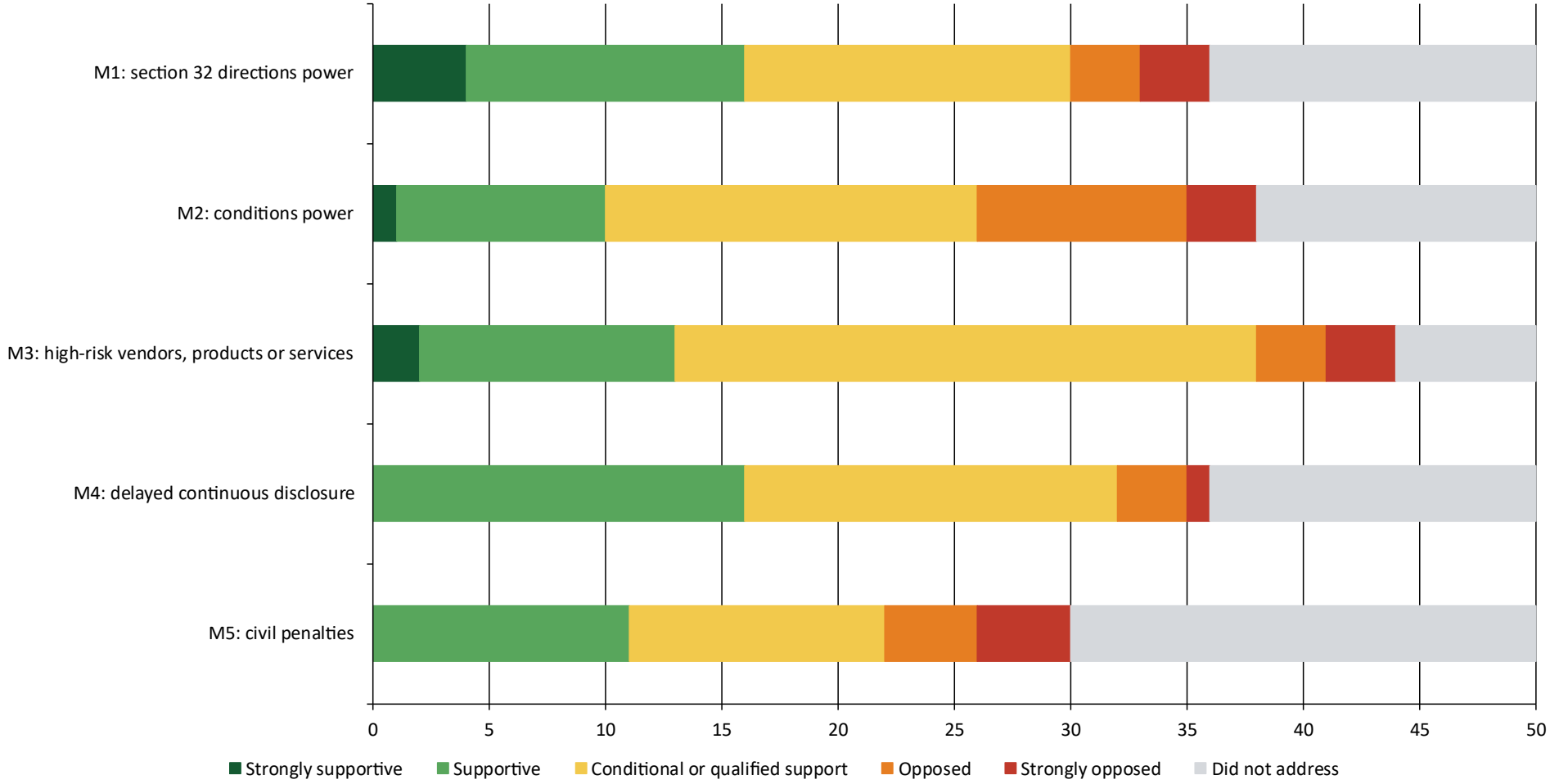
- As written submissions generally did not provide quantified cost information, the Department undertook targeted Impact Analysis consultations in May 2026 and accepted a small number of late or follow-up materials. This additional engagement tested implementation impacts, activity changes, cost assumptions, implementation timeframes, business-as-usual overlap, service continuity, competition effects and distributional impacts.

Engagement summary: 25 March 2026 – 1 May 2026	
Total number of online engagements	4
Total number of attendees at online engagements	757
TISN engagements	2
Total number of attendees at TISN engagements	603
Public online engagements	2
Total number of attendees at public online townhalls	154

Overview of all engagements: 25 March 2026 – 21 May 2026	
1 April 2026	Out-of-Session meeting of the National Cyber Security Committee (NCSC)
7 April 2026	Public Town Hall
15 April 2026	TISN Cross-Sector Group Briefing
17 April 2026	TISN Government Sector Group Briefing
20 April 2026	Public Town Hall
29 April 2026	Briefing for State and Territory Governments
15-21 May 2026	Series of bilateral meetings with responsible entities and industry peak bodies

Sentiment analysis

Stakeholders generally recognised the need for effective national security tools to respond to serious risks affecting critical infrastructure. Many submissions supported strengthening the Ministerial Directions framework, particularly for systemic, fast-moving or vendor-level risks that may not be fully managed by individual entities acting alone. Stakeholder views were often conditional rather than opposed, with submissions commonly seeking assurance that the powers would remain exceptional, proportionate and supported by consultation, clear thresholds, legal certainty, realistic transition pathways and practical guidance. The chart below shows sentiment by measure and separately identifies submissions that did not address a particular measure.



***Methodology**: The Department assessed each submission against each proposed measure, based on the substance of the views expressed. Sentiment is presented as supportive or strongly supportive, conditional or qualified support, opposed or strongly opposed, or did not address. "Conditional or qualified support" includes submissions that supported the policy objective or measure in principle while seeking safeguards, clearer limits, guidance or implementation changes. "Did not address" is shown separately for transparency. The analysis is qualitative and should be read as an indication of views expressed through consultation, not as a statistically representative survey of all critical infrastructure entities, sectors or members of the public.*

Feedback summary

Stakeholders recognised that Australia's critical infrastructure faces serious and evolving national security risks, including cyber threats, supply-chain compromise, high-risk vendor access, offshore support arrangements, governance vulnerabilities, and risks arising from ownership, control or influence arrangements. Many submissions accepted that some risks may be systemic and fast-moving and may not be capable of being fully managed by individual entities acting alone.

Support for the proposed reforms was generally conditional. Stakeholders sought assurance that the powers would remain exceptional and proportionate, with clear thresholds, security advice, consultation where practicable, consideration of operational impacts, legal certainty for good-faith compliance, realistic implementation pathways and practical guidance.

Overall themes

Exceptional and proportionate use

What stakeholders said

Stakeholders supported national security intervention where a serious risk cannot be adequately addressed through voluntary action or existing regulatory mechanisms. They asked that the powers remain exceptional and that decision-making account for commercial, economic, social, safety and operational impacts.

How the reforms respond

The reforms preserve the last-resort character of Part 3. The powers are tied to serious national security or material asset-security risks, and their use is subject to necessity, proportionality, consultation and mandatory consideration of relevant impacts.

Consultation and coordination

What stakeholders said

Stakeholders accepted that urgent or sensitive national security circumstances may limit consultation. They nevertheless sought early engagement where practicable, including with affected entities, relevant Commonwealth regulators, State and Territory governments, market bodies and sector specialists.

How the reforms respond

The reforms strengthen consultation before Part 3 powers are used. The amended section 32 power and the new conditions power add Commonwealth consultation, while vendor-risk and delayed disclosure directions include consultation models tailored to the entities, regulators and markets most likely to be affected.

Legal certainty and good-faith compliance

What stakeholders said

Stakeholders raised concerns that compliance with a lawful direction could affect contracts, directors' duties, customer commitments, overseas law, State and Territory legislation, market rules or sector-specific regulatory obligations.

How the reforms respond

The reforms provide legal certainty for entities that act in good faith to comply with lawful directions. The design includes protection from damages actions for good-faith compliance with new conditions directions, vendor-risk directions and delayed disclosure directions. For vendor-risk directions, the reforms

also address contractual and civil liability issues where compliance requires changes to existing commercial arrangements.

Practical implementation and service continuity

What stakeholders said

Stakeholders stressed that directions must be technically feasible and capable of implementation without creating greater operational, safety or service-continuity risks. These concerns were strongest for operational technology, telecommunications networks, data centres, energy systems, water infrastructure and financial market infrastructure.

How the reforms respond

The reforms require practical impacts to be considered before a direction is given, including costs, customer and service impacts, competition, supply-chain effects, alternatives, timeframes and regulatory overlap. For vendor-risk directions, the framework also supports transition timeframes, phased implementation and compensating controls where immediate removal or replacement is not feasible.

Implementation guidance

What stakeholders said

Stakeholders consistently asked for practical guidance and worked examples. Submissions sought clearer explanation of thresholds, consultation processes, mandatory considerations, direction lifecycles, compensating controls, legal protections, vendor-risk scenarios and delayed disclosure scenarios.

How the reforms respond

The Department will develop guidance for industry and government to support implementation of the reforms. Guidance will explain how the powers may operate in practice, what information may be sought from entities, how consultation may occur, how mandatory considerations will be applied, how implementation issues may be managed, and how entities may seek clarification, variation or revocation of a direction.

Guidance will include worked examples for the most complex scenarios, particularly vendor-risk directions and delayed disclosure. These examples will help boards, executives, vendors and regulators understand expected processes and safeguards, while avoiding disclosure of sensitive operational, commercial or security information.

Feedback by measure

Measure 1: amendments to the existing section 32 directions power

What stakeholders said

Stakeholders expressed mixed views on changes to the existing section 32 directions power. Some supported making the power more operationally usable, particularly where a time-sensitive national security risk cannot be addressed through voluntary action or another regulatory scheme. These stakeholders generally accepted replacing the Adverse Security Assessment requirement with tailored ASIO advice, provided security expertise, high thresholds, proportionality, consultation and review safeguards are retained.

Other stakeholders considered the Adverse Security Assessment requirement and the current regulatory exhaustion test to be important safeguards. They were concerned that recalibrating those requirements

could make it harder for affected entities to understand the basis for a direction or could allow SOCI powers to be used before sector-specific mechanisms have been properly considered.

How the reforms respond

The reforms retain security advice as a central safeguard. Before exercising the amended section 32 power, the Minister must obtain and consider ASIO advice directed to the relevant entity or asset. This preserves a clear role for security expertise while allowing the Minister to weigh that advice alongside regulatory, economic, commercial, social and operational considerations.

The reforms also retain the last-resort character of section 32. The Minister must still be satisfied that a direction is reasonably necessary to eliminate or reduce the relevant risk, and that reasonable steps have been taken to negotiate in good faith with the entity before a direction is given.

The reforms keep other regulatory frameworks at the centre of decision-making. Rather than operating as a hard legal bar, the availability of another Commonwealth, State or Territory regulatory system becomes a mandatory consideration. The Minister must consider whether another regulatory system could more effectively address the identified risk before giving a direction.

This responds to concerns about duplication while preserving the ability to act where another framework is not designed for the national security risk, is unlikely to produce an adequate outcome, or cannot operate within the required timeframe. The reforms also expand Commonwealth consultation so that relevant Ministers and departments with responsibility for the affected sector are consulted before a Part 3 direction is given.

Measure 2: conditions power

What stakeholders said

Stakeholders recognised that ownership, control, influence and governance arrangements can create national security risks for critical infrastructure. Examples included foreign ownership or influence, parent-company influence, offshore administration, access to sensitive information, board or committee decision-making, insider threats and governance failures affecting critical systems or services.

Some stakeholders supported a conditions power as a more tailored response than a broad direction to do, or refrain from doing, an act. Others questioned whether a new power was needed where existing frameworks already regulate foreign investment, corporate governance, hosting, telecommunications, personnel security or prudential risk. Stakeholders asked that any conditions be targeted, proportionate, reviewable and capable of variation where risk changes.

How the reforms respond

The reforms create a dedicated conditions power to address a specific gap in the existing framework. Other regimes may regulate foreign investment, corporate governance, prudential risk, hosting or telecommunications security, but they do not always provide a practical mechanism to address ownership, control, influence or governance risks that emerge after existing approvals, sit across multiple regimes, or cannot be sufficiently managed through voluntary action.

The power is confined to material national security risks affecting critical infrastructure assets. It is not a general corporate governance power. Before imposing conditions, the Minister must be satisfied that the relevant arrangements could give rise to a risk that is prejudicial to security, or could materially affect the operation, availability, integrity, reliability, confidentiality or security of the asset, and that conditions are reasonably necessary to mitigate or eliminate that risk.

The reforms also respond to concerns about duplication and proportionality. The Minister must consider whether another Commonwealth, State or Territory regulatory regime could more effectively address the risk, consult affected entities and relevant Ministers, and consider any representations received. Conditions can

be tailored to the risk, including through access, information-handling, personnel security, governance, cyber security, segregation, audit or reporting requirements.

Conditions are also subject to ongoing review. A direction must be reviewed within 12 months and at least every 24 months after that, and may be varied or revoked where circumstances change. Entities may also trigger review by notifying the Minister of a material change relevant to the risk. Legal certainty is supported by written directions, implementation periods, reporting requirements and protection from damages actions for good-faith compliance.

Measure 3: restrictions on high-risk vendors, products or services

What stakeholders said

Stakeholders accepted that high-risk vendors, products, equipment, services or technologies can create systemic risk where they are widely used across critical infrastructure, have privileged access, support critical systems, or are affected by foreign ownership, foreign legal obligations, supply-chain compromise, technical vulnerabilities or insecure service arrangements.

Stakeholders were particularly concerned about directions requiring replacement or remediation of existing systems. Operators in operational technology-intensive sectors emphasised that changes may require outage windows, redesign, testing, safety validation, staged deployment and regulatory approval. Data centre, cloud and telecommunications stakeholders raised customer impacts, hosted workload dependencies, global architecture constraints, service level agreements and continuity of essential services.

Stakeholders also raised competition and market concerns, including supplier concentration, supply-chain bottlenecks, contractual impacts and increased costs. They sought clear criteria, sector-specific consultation, reasonable transition timeframes, procedural fairness for affected entities and vendors, and legal certainty where compliance affects existing commercial arrangements.

How the reforms respond

The reforms create a dedicated vendor-risk directions power to address systemic risks that cannot be managed effectively through entity-by-entity directions alone. The power applies where risks arise from specified vendors, products, equipment, services or technologies used in connection with critical infrastructure assets, including risks that affect a single asset, multiple assets, an asset class, a sector or a defined class of responsible entities.

The power is confined by clear thresholds. The Minister must be satisfied that the specified vendor, product, equipment, service or technology poses a material risk that is prejudicial to security, or a material risk to the continued availability, integrity, reliability or security of one or more critical infrastructure assets. The Minister must also be satisfied that a direction is necessary to mitigate or eliminate that risk.

The reforms respond to implementation and service-continuity concerns by allowing directions to be tailored to the risk. A direction may require an entity to cease or reduce use, refrain from future procurement, remove, disable, isolate, segment or remediate technology, modify the way a service is used, or implement compensating controls where immediate removal is not feasible.

Before issuing a direction, the Minister must consider operational and market impacts, including economic and social implications, supply-chain effects, end-user impacts, competition, asset availability or reliability, alternative vendors or technologies, implementation timeframes, and whether another regulatory regime could more effectively address the risk.

The reforms also provide procedural fairness for affected entities and vendors. For named directions, the Minister must consult affected entities and, where reasonably practicable, affected vendors. For class directions, the Minister must publish a consultation notice inviting submissions from affected entities, affected vendors and other interested parties, and consult relevant Commonwealth, State and Territory Ministers and agencies.

Vendor-risk directions can be varied, revoked and reviewed so they remain necessary and proportionate as circumstances change. The Minister must revoke a direction if it is no longer required to address the identified risk, and affected entities or vendors may seek review where there has been a material change to the specified risk. Legal certainty is supported by good-faith liability protection, including where compliance affects existing commercial or contractual arrangements.

Measure 4: delayed disclosure

What stakeholders said

Stakeholders generally supported a narrow mechanism to delay public disclosure in rare cyber incidents where immediate disclosure could prejudice national security or incident response. They recognised that premature disclosure may alert a threat actor, accelerate malicious activity, compromise containment or remediation, reveal vulnerabilities, or undermine a coordinated government response.

Market-facing stakeholders raised concerns about market integrity, false market risk, insider trading, confidentiality, regulator coordination and legal certainty for directors and disclosure committees. Stakeholders also sought clarity on what confidential communications would remain permitted during a delay.

How the reforms respond

The reforms introduce a targeted mechanism allowing the Minister for Home Affairs to direct a SOCI-regulated entity not to make public disclosure of a specified cyber security incident for a limited period where disclosure would pose a risk to Australia's national security. The power applies where the entity has, or is reasonably likely to have, continuous disclosure obligations under Chapter 6CA of the Corporations Act or the ASX Listing Rules.

The mechanism applies only to public disclosure of the specified cyber security incident. It does not suspend SOCI cyber incident reporting obligations, notifiable data breach obligations or necessary confidential communications for incident response, regulator engagement, legal advice, audit, insurance, contractual coordination or other compliance purposes.

The proposed design responds to market integrity concerns through mandatory insider trading controls. The decision-maker must consider investor impacts, trading in the entity's securities, confidence in the market, the proposed duration of the delay, the risk of improper trading and the adequacy of trading controls. Every direction must require the entity to identify relevant persons, notify them of a trading blackout, take reasonable steps to prevent trading, and notify ASIC.

The decision-maker must consult Treasury and ASIC on market integrity, investor protection, continuous disclosure and insider trading issues, and ASD on the national security and operational consequences of premature disclosure. The affected entity must also be consulted where the direction is not entity-initiated and consultation is practicable.

The delay mechanism is time-limited. An initial direction may operate for up to 30 days, with a further extension of up to 30 days if the national security risk continues, and a final extension of up to 60 days in extraordinary circumstances. The total duration of a delay under a single direction cannot exceed 120 days. A direction may be revoked if the national security grounds no longer exist and automatically ceases if information about the incident becomes generally available.

Measure 5: increased civil penalties

What stakeholders said

Measure 5 attracted less detailed operational feedback than the other measures because it does not itself require systems, supplier, governance or disclosure changes. Stakeholders generally understood that the substantive compliance burden arises from the underlying direction rather than the maximum penalty setting.

Some stakeholders supported higher maximum penalties as a deterrent for serious non-compliance. Others were concerned that higher penalties could undermine the cooperative character of the SOCI regime unless enforcement recognises good-faith efforts, technical feasibility, safety risks and realistic transition requirements.

How the reforms respond

The proposed penalty settings are directed to serious non-compliance with lawful national security directions. They are intended to provide a credible deterrent where non-compliance could have significant consequences for national security, critical infrastructure resilience or essential service continuity.

The penalties are maximums and do not create a separate operational burden. The practical compliance task will continue to be determined by the direction itself, including any implementation period, transition arrangements or technical requirements.

The reforms preserve proportionate, risk-based enforcement. Compliance decisions will take account of technical feasibility, safety, service continuity, reliance on third parties, implementation timeframes and good-faith efforts to comply. This supports stronger deterrence while maintaining the cooperative character of the SOCI regime.