NSW Telco Authority Submission

Ministerial Direction Powers -SOCI Act

April 2026

Ministerial Directions Powers Submission

Background

Following the recommendations from the Independent Review Final Report February 2026, the Department of Home Affairs (DHA) is progressing the first tranche of initiatives, which are primarily directed at reducing complexity and improving the agility and responsiveness of the *Security of Critical Infrastructure Act 2018* (SOCI Act), including through legislative reform.

The Minister for Home Affairs is opening consultation and seeking submissions on the proposed changes from 30 March 2026 to 1 May 2026:

1. Industry views on a potential package of five (5) targeted measures to enhance the Ministerial directions powers under Part 3 of the SOCI Act. As set out in the Consultation Paper: Proposed amendments to the Ministerial Directions Powers in Part 3 of the SOCI Act (453KB PDF).

All submissions will be provided to the Minister for Home Affairs for consideration by 1 May 2026 and lodged via the submission's portal on the DHA website.

The proposed amendments will apply to NSW Telco Authority (NSWTA) as a responsible entity for critical infrastructure assets, including telecommunications. As such, NSWTA is invited to provide a submission in response to the proposed reform.

This initiative will allow the Minister to weigh all relevant factors, including economic, commercial, social and regulatory considerations, alongside national security risks, to support responses that are proportionate, transparent, defensible and aligned with whole-of-government objectives.

Current Obligations

The following provides a summary of the key obligations under the SOCI Act, with which NSWTA is currently aligned and meeting regulatory expectations.

Detail Register of Critical Infrastructure Assets (Part 2) Responsible entities and direct interest holders must provide the Critical Infrastructure Security Centre (CISC) (within the Department) with required operational, ownership, and interest and control information.

Mandatory Cyber Security Incident Reporting (Part 2B) Responsible entities must report actual or imminent cyber security incidents to the Australian Signals Directorate (ASD).
Relevant impact: Within 72 hours, they must provide a report on impacts on asset availability, integrity, reliability, or confidentiality of information.
Significant impact: Within 12 hours they must provide a report on whether an incident has materially disrupted the provision or availability of essential goods or services.

Critical Infrastructure Risk Management Program (CIRMP) (Part 2A) - Responsible entities in 13 designated asset classes must adopt, maintain and comply with a written CIRMP that takes an all-hazards approach across four (4) key vectors:

- physical security and natural hazards
- personnel hazards
- supply chain hazards
- cyber security and information security hazards.

Key requirements: The entity is obliged, among other things, to:

- identify and mitigate material risks,
- comply with a designated or equivalent cybersecurity framework (including the AAESCSF) and meet specified maturity levels, and
- provide annual reporting to regulators within 90 days after the financial year end.

The CISC may direct a responsible entity to vary its CIRMP to address a serious deficiency that poses a material risk to national security, Defence, or social or economic stability.

DHA Proposed Amendments

Ministerial Directions Powers

The proposed five (5) measures would enhance the Ministerial directions powers under Part 3 of the SOCI Act and provide greater flexibility and precision in managing serious national security risks to critical infrastructure, while maintaining clear safeguards and accountability. For consultation purposes, the measures are set out separately to highlight the distinct issues each is intended to address and invite targeted, granular feedback.

The following five (5) targeted measures include:

1. Amendments to the existing directions power in section 32 – replace the existing Adverse Security Assessment (ASA) requirement, introduce a limited carve-out from the prescribed administrative action framework, recalibrate the 'regulatory exhaustion' requirement,
2. Conditions Power - Access, information-handling, and personnel security controls, Board, governance and decision-making safeguards, Cyber security baselines and uplift, Transparency, oversight and audit.
3. Restrictions on the use of high-risk vendors, products or services - a vendor-risk direction power to enable coordinated action where a specific vendor or its products, equipment, services or technologies, present a material risk to national security. This power would ensure systemic supply chain vulnerabilities can be managed consistently across affected critical infrastructure entities and sectors.
4. Delay continuous disclosure requirements - Section 111AT of the Corporations Act grants ASIC the power to exempt entities from disclosure obligations under the Corporations Act. Insert a new directions power into the SOCI Act to allow the Minister for Home Affairs to direct an entity to not publicly disclose the existence of the cyber incident for a prescribed period.
5. Increased civil penalty provisions - increasing the maximum civil penalty for non-compliance with a Ministerial direction under Part 3 to 2,000 penalty units, aligning it with the enforcement framework already operating in Part 2D of the SOCI Act for carriers and carriage service providers.

NSWTA Submission – Ministerial Directions Powers

NSWTA consulted a range of internal stakeholders on the proposed five (5) measures and consolidated the feedback below, including the anticipated organisational impacts.

NSWTA's feedback is provided in the context of a responsible entity with demonstrated compliance maturity and is framed to support the application of the proposed measures in a risk-based, proportionate and operationally achievable manner.

1. Amendments to the existing directions power in section 32
    - Replacing the current Adverse Security Assessment (ASA) requirement with ASIO advice would speed up the Minister's ability to request information on material risks and evidence of mitigation.
    - The change would require closer monitoring of the critical infrastructure risk treatment plan and audit recommendations; the Risk team supports it, as it would drive more proactive risk management.
    - A sufficient grace period would be required to implement the amendments, commensurate with the nature and urgency of the risk being addressed.
    - The approach would reduce delays in time-sensitive situations but would require strong organisational readiness to respond quickly (people, facilities, vendor access, communications, record keeping).
    - Procedural documents would need to be updated.
2. Conditions Power
    - No major cyber uplift identified. The proposed reforms don't indicate a material uplift beyond existing cyber security obligations, noting the potential for duplication arising from additional directions.
    - Vendor cyber security assessments are already undertaken for every vendor.
    - Potential WHS/psychosocial impacts: The changes could increase workload, accountability, and role expectation changes, creating psychosocial WHS risks; any guidance should explicitly address these impacts.
    - It is appropriate for the Minister to impose conditions where ownership, control or governance arrangements create a material risk
    - Amendments would require strengthening (uplifting) cyber security and ICT governance.

3. Restrictions on the use of high-risk vendors, products or services
    - Need clarity on who will be responsible for assessing and classifying vendors as "high risk."
    - Support the amendment as it will push business units to strengthen supplier due diligence.
    - A review of vendor governance structures is needed to properly identify and manage supply chain risks.

4. Delay continuous disclosure requirements

- Support the proposed amendment. This new measure will allow for the protection of sensitive/confidential info not to be released.

5. Increased civil penalty provisions

- New requirements would need to be added to vendor contracts; assess impacts on existing contracts and scheme agreements.
- This is a significant increase in penalty units.
- Consideration is required on business continuity and operational impacts should the penalties impact the service delivery.

NSWTA Submission – CIRMP Rules

NSWTA assets are registered as telecommunications assets; accordingly, they would not be subject to the proposed enhanced CIRMP requirements and would instead remain governed by the existing requirements under the SOCI Act.