Feedback Submission – SOCI Act 2018

Feedback Submission – Independent Review of the Security of Critical Infrastructure Act 2018

To: Department of Home Affairs Independent Review Panel
From: Transport for NSW
Date: 22 December 2025

Decision maker

Thank you for the opportunity to provide feedback on the Independent Review of the Security of Critical Infrastructure Act 2018 (SOCI Act). We appreciate the Commonwealth's efforts to strengthen the resilience of critical infrastructure and welcome the consultation process.

As part of this submission, we have compiled recommendations from Transport for NSW stakeholders to address practical challenges and improve clarity, efficiency, and alignment with industry best practices. These recommendations reflect operational realities across transport assets and interdependencies with other sectors.

Executive summary

The recommendations outlined in this submission have been consolidated from extensive stakeholder feedback and are presented in summary form below, with the full list of comments and detailed recommendations provided below. These recommendations aim to strengthen the Security of Critical Infrastructure Act 2018 by addressing practical challenges and improving clarity, efficiency, and resilience across critical sectors.

1. Is the SOCI Act achieving its intended objectives?

Partially, but with gaps.

The Act aims to strengthen the security and resilience of critical infrastructure, and stakeholders acknowledge its importance. However, feedback indicates that ambiguity in definitions (e.g., "material risk," "hazard," scope of critical assets) and lack of clear guidance on frameworks and compliance requirements hinder full achievement of objectives. Additionally, duplication of state and federal obligations creates inefficiencies that detract from the Act's effectiveness.

2. Is the SOCI Act functioning as intended?

Not fully.

While the Act establishes obligations for asset owners, its implementation is uneven due to unclear terminology, overlapping compliance requirements, and insufficient templates or maturity pathways for CIRMPs. The Act also places disproportionate cybersecurity responsibility on asset owners rather than sharing it with product suppliers, which is inconsistent with best practice (e.g., ASD's Secure by Design principles).

3. Is the SOCI Act having any unintended consequences?

Yes.

Compliance Burden: Duplication of reporting obligations between SOCI and state policies (e.g., Cyber NSW) increases administrative overhead.

Overreach in Definitions: Broad definitions (e.g., critical telecommunications networks) capture internal networks not used for public services, creating disproportionate obligations for some entities.

Ambiguity in Risk Management: Lack of clarity on "material risk" and inconsistent use of "risk" (hazard-based interpretation) leads to confusion and potential misalignment with ISO 31000 standards.

4. Are there new or emergent threats the SOCI Act is unable to manage in its current form?

Yes.

Emerging Technologies: Current definitions do not adequately account for future transport technologies or cross-sector interdependencies.

Supply Chain Complexity: Guidance does not sufficiently address tiered supply chain risks beyond "major suppliers," leaving gaps in managing vulnerabilities introduced by third-party operators.

Framework Fragmentation: Multiple cyber frameworks referenced without clear compliance expectations create uncertainty in addressing evolving cyber threats effectively.

Summary of comments received internally

Clarification of Definitions and Scope

- The Act and Rules do not clarify how obligations apply when the same asset or component is classified under multiple critical asset categories across different sectors (e.g., a telecommunications network that is also part of a public transport asset).
- The current definition of a critical telecommunication network is overly broad, capturing all networks owned by a carrier, including private internal networks not used to supply public carriage services. This results in disproportionate compliance obligations for entities. The suggestion is to limit the application of certain parts of the Act (Parts 2, 2A, and 2B) through rules so that internal networks are excluded.
- The definition of public transport critical assets appears to apply only to "closed" systems such as metro, rail, and light rail. There is uncertainty about whether it also applies to "open" systems like motorways or roadways, for example, the motorway network operated by Transurban.
- The Act does not define key terms such as "hazard" or "material risk." While these are explained in the SOCI CIRMP, they should also be included in the Act for clarity, especially since SOCI Rules do not apply to all sectors and these terms appear in other sections.
- Future-proof definitions to capture emerging transport technologies and mandate cross-sector interdependency assessments.

Reduce Compliance Duplication

- The SOCI Act and its regulations duplicate existing NSW State legislative and policy obligations, such as cyber incident reporting. This duplication creates unnecessary compliance burden. The recommendation is to either remove duplication or implement a simplified compliance mechanism.
- Establish a central reporting agency for critical infrastructure incidents to reduce reporting burdens. Current SOCI legislation and mandatory state cybersecurity policies require

separate incident reporting to both federal (ACSC under SOCI) and state (Cyber NSW) agencies. This duplication creates inefficiencies and increases the reporting burden.

Enhance Guidance and Frameworks

- Industry has expressed a strong preference for using the NIST Cybersecurity Framework (CSF) to meet Critical Infrastructure Risk Management Program (CIRMP) requirements. However, the framework does not appear to be explicitly permitted for meeting the Transport Sector Risk Management Program (TSRMP) obligations for carriers.
- The CIRMP references multiple cyber and information security frameworks, but these frameworks vary significantly in purpose and structure (e.g., control-based standards, risk management systems, maturity models). This creates ambiguity around what it means to "comply with a framework." Clear guidance is needed to define compliance expectations across these differing approaches to ensure consistency and assess ability.
- Current SOCI obligations lack comprehensive guidance and standardised reporting templates, making it difficult for organisations to interpret requirements and achieve compliance. For example, entities submitting a Critical Infrastructure Risk Management Program (CIRMP) only receive high-level descriptions without detailed instructions or templates.
- Clarify the meaning of "material risk" within CIRMP requirements, as current guidance is vague and only references likelihood and impact without defining thresholds or criteria. This ambiguity creates uncertainty about whether "material risk" refers to any risk requiring management, risks above a certain level, or those within the four legal categories (cyber, people, physical, supply chain). To ensure consistency and alignment with best practice, adopt the ISO 31000 definition of "risk" and provide clear guidance on assessing and categorising material risks.
- Current guidance focuses on principles and desired outcomes but lacks practical direction. Recommending established frameworks (without making them mandatory) would help responsible entities meet obligations more effectively and consistently.
- The SOCI Act currently places most cybersecurity obligations on asset owners and operators, while product suppliers have minimal responsibilities. This creates an imbalance, as manufacturers are better positioned to improve product security and reduce risks for customers, consistent with ASD's *Secure by Design* principles.

Supply Chain Risk Management

- Current guidance on supply chain risk management focuses primarily on "major suppliers" but lacks detail on how deep assessments should go (e.g., Tier levels). More comprehensive principles and processes would help agencies implement necessary controls, including contractual agreements, especially when third-party operators manage critical infrastructure.
- Recommend established frameworks for supply chain risk management without mandating them.

Government Support and Engagement

- Clear guidance is needed on how responsible entities should engage with state and federal agencies during incident remediation. While the SOCI Act grants federal agencies authority to assist, request information, and direct actions, the NSW Cyber Security Emergency Plan also empowers the State Emergency Operations Controller (SEOCON) to enforce monitoring and reporting protocols. Without clear engagement protocols, entities face uncertainty in aligning processes with mandatory policies and legislation.

- Offer government-led training, certification, and exercise support tailored to transport interdependencies.

Incident Reporting Improvements

- Clarify thresholds for “significant” vs. “relevant” impacts in transport scenarios.
- Enable staged reporting for complex incidents.

We trust these recommendations will assist in shaping a more practical and effective regulatory framework. Please do not hesitate to contact us for further discussion or clarification.

[redacted].