Microsoft

22 December 2025

Dr Jill Slay AM
Independent Reviewer of the SOCI Act
SOCI.Independent.Review@homeaffairs.gov.au

Dear Dr Slay,

Microsoft welcomes the opportunity to provide a submission to the independent review of the *Security of Critical Infrastructure Act 2018* (Cth) (SOCI Act). Having operated in Australia for over 40 years, Microsoft is deeply committed to strengthening the nation's cyber resilience, and we recognise the special responsibility we have as a provider of data services that underpin the governments, industries and broader society of Australia.

In our view, Australia remains a leading jurisdiction in regulating critical infrastructure security. The SOCI Act embeds proactive risk management, mandatory incident reporting, cyber security preparedness and transparency measures, and the legislation is underpinned by a comprehensive approach to public-private collaboration and capacity building led by the Department of Home Affairs. This review provides an important opportunity to build on these strong foundations, refine the framework, and ensure Australia remains at the forefront of global best practice in a rapidly evolving threat environment.

Notwithstanding the strengths of the existing law, there are clear opportunities for improvement. Based on our global experience, we recommend the review focus on the following priorities:

1. Strengthening the resilience of critical infrastructure to the future threat environment
2. Simplifying and clarifying obligations to uplift maturity across sectors
3. Aligning obligations with international best practice
4. Maintaining a proportionate compliance and enforcement regime

1. Strengthening the resilience of critical infrastructure to the future threat environment

Microsoft processes over 100 trillion security signals per day, giving us unparalleled insight into cyber threats. Our latest Digital Defense Report shows critical infrastructure in Australia and across the globe faces an intensifying cyber threat environment and remains a prime target for both nation-state actors and cyber-criminals aiming to disrupt society or reap large profits. At the same time, identity-based attacks are surging, AI is accelerating both cyber-attacks and defence, and there is a looming encryption challenge posed by quantum computing.[1]

In this environment, it is critical obligations under the SOCI Act continually evolve to strengthen resilience to emerging threats, as recognised in the review's Terms of Reference.

[1] Microsoft Digital Defense Report 2025

Fortunately, the SOCI Act's adaptable, principles-based structure provides a strong foundation to handle these challenges. As new technologies emerge over time, the law should not attempt to codify detailed requirements for each, as they risk quickly becoming obsolete or even counterproductive. The review should first explore whether the Act's existing regulatory levers are sufficient to address emerging risks and harness advanced security capabilities such as:

- **AI-enabled threats and defences:** Adversaries are already exploiting AI to increase the speed, scale and sophistication of their attacks. This trend will only accelerate. AI systems have also become an attractive target for cyber-attacks. On the other hand, AI is also a game-changer for cyber defence, from machine learning systems that detect anomalies, to AI-driven automation that can triage and respond to incidents at machine speed. The SOCI Act framework should take an outcomes-based approach to encouraging responsible critical infrastructure entities to manage AI risks responsibly while recognising the use of AI-enabled cyber defences as part of a robust risk management approach.
- **Post-quantum cryptography (PQC):** Governments worldwide have recognised the threat posed by quantum computing to traditional encryption and are setting ambitious timeframes to transition to PQC. The same level of urgency is required in critical infrastructure. This is a multi-year and complex transition process, and systems are already vulnerable today as malicious actors employ "harvest now, decrypt later" strategies. The Government can aid critical infrastructure entities to mitigate the risk of quantum computing, for instance, by encouraging an inventory of cryptographic assets and the development of transition plans to new algorithms.
- **Modernising legacy IT:** The use of outdated legacy infrastructure and software is widespread across government and critical infrastructure. This legacy IT often lacks vendor support, accumulates unpatched vulnerabilities, and is incompatible with modern security standards[2]. These risks are magnified in critical infrastructure, where operational continuity and public safety are paramount. Modernising legacy systems, promoting cloud migration and incentivising the adoption of security-by-design and security-by-default technology products should be considered central to risk management, and will also be necessary to underpin future AI and PQC adoption.

Rather than addressing each threat or technological shift on a case-by-case basis, an alternative approach could be to move towards a "resilience-by-design" requirement. As highlighted in Microsoft's 2025 Digital Defense Report, resilience must be engineered into systems, supply chains, processes and governance from the outset, not bolted on after the fact. Resilience-by-design encompasses both technical and organisational measures to anticipate, withstand, recover and adapt to a wide range of cyber-physical threats (see figure 1).

Recommendation 1: Leverage the SOCI Act's existing adaptable, principles-based structure to address emerging threats to critical infrastructure security, such as AI, quantum computing and outdated legacy IT, rather than introducing prescriptive requirements that risk quickly becoming obsolete or counterproductive. This could be supported by the introduction of a "resilience-by-design" requirement that recognises the need to shift from a purely defensive posture to one that recognises resilience as a core design principle to anticipate, withstand, recover and adapt to a wide range of cyber-physical threats.

[2] Unlocking the productivity dividend of digital government

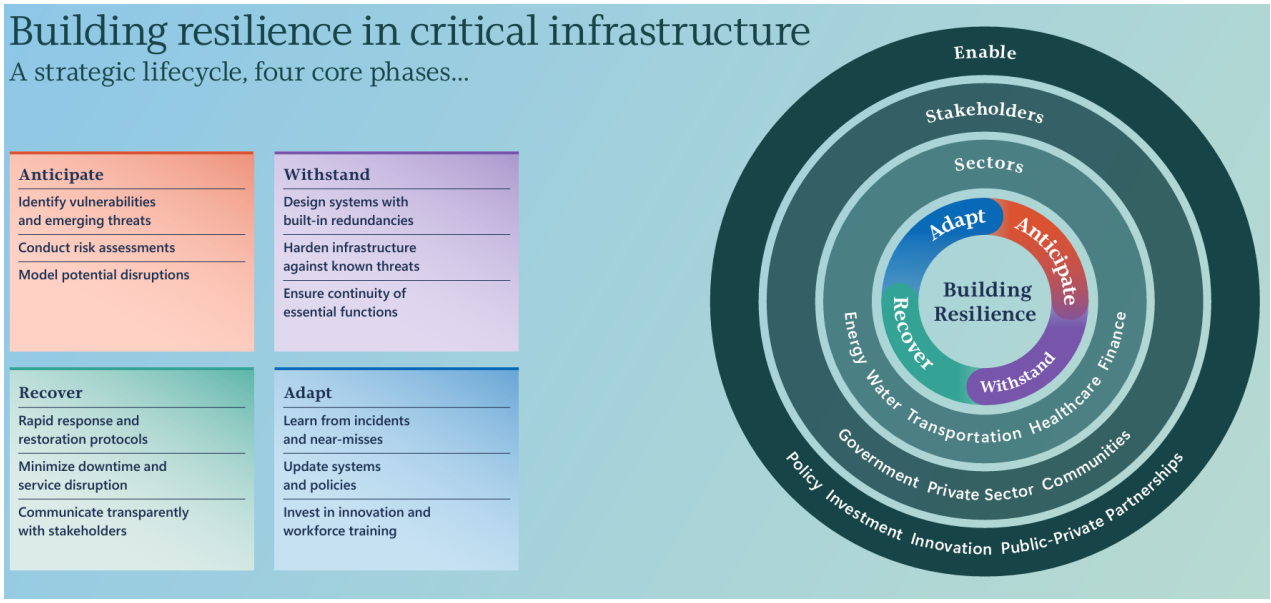

Figure 1: Microsoft framework for "resilience-by-design"

2. Simplifying and clarifying obligations to uplift maturity across sectors

The SOCI Act is widely regarded as a global exemplar of critical infrastructure regulation. Over time, however, industry has encountered growing complexity in compliance. Bolt-on amendments, overlapping obligations, ambiguous definitions, and evolving guidance have at times created confusion for responsible entities. Microsoft believes the review can identify ways to simplify the Act's requirements and provide greater clarity, making it easier for organisations to comply and focus on security outcomes. In particular:

- We support the introduction of a more tailored, risk-based approach to supporting cyber maturity on a sector-by-sector basis. Entities across different sectors, such as utilities, banks, universities, and cloud providers, face different threat profiles and have reached different security maturity levels. Evaluating each sector's cyber maturity and developing sector-specific uplift plans is a sensible step. However, it will be critical for this to be accompanied by meaningful engagement structures to ensure any sector-specific measures are fit-for-purpose, feasible and truly risk-aligned.
- To help reduce regulatory duplication:
    - We endorse increased collaboration among critical infrastructure and security regulators. A coordinated approach could help reduce duplication, harmonise definitions, and streamline compliance. Establishing a Cyber Regulators Forum could formalise this effort and improve regulatory clarity.
    - The Government should retain existing exemptions for the CIRMP requirement for organisations holding a Strategic Hosting Certification under the Hosting Certification Framework. This exemption is critical to avoid regulatory duplication and, related to the first point above, reflect different risk profiles and cyber maturity levels.
- The scope of notifiable incidents intended to be caught under the legislation is unclear in practice, particularly when considered alongside the SOCI Act's broader all-hazards framework. Further clarification and guidance would be welcomed to ensure that

availability incidents resulting from non-malicious technical failures, such as outages or engineering defects, are excluded from the definition of reportable cyber security incidents. For example, some case studies in the official CISC Mandatory Cyber Incident Reporting Guide are currently ambiguous and may create confusion.

- There is no specific form to submit an annual report under Part 2AA of the Act, only the form under Part 2A which is relevant to critical infrastructure which should be covered by a CIRMP. We suggest separate prescribed forms for each of the Part 2A and Part 2AA reports to improve clarity and enhance SOCI Act reporting requirements.
- There is a 30-day requirement to update the Asset Registry for relevant changes, but changes which may fall under a 'notifiable event' in the data sector typically occur less than once per year. Additionally, the details required in the prescribed Asset Registry form go over and above what constitutes 'operational information' in the SOCI Act, meaning the requirement to update the information provided in the Asset Registry form is potentially triggered more often than arguably intended by the SOCI Act. In line with the proposal to adopt tailored approaches to different sectors, an extended timeframe for the data sector would maintain relevance while reducing administrative burden.
- Finally, in line with our recommendation to adopt a more tailored approach to different sectors, the last resort Government Assistance Powers in the Act require review. While these powers apply only in exceptional circumstances and are supported by a range of safeguards, we continue to hold concerns about the appropriateness of these powers being exercised over sophisticated hyperscale cloud environments. Introducing third-party software or mandating direct intervention in complex cloud systems risks unintended consequences, including service disruption and the creation of new vulnerabilities. We therefore encourage the consideration of an exemption mechanism for entities that demonstrate mature cyber security capabilities, a history of cooperation with government, and robust incident response protocols. This would allow the Government to focus its intervention powers where they are most needed, while recognising the unique risk profile and operational sophistication of certain providers.

Recommendation 2: Adopt targeted reforms to simplify and clarify SOCI Act obligations in a way that will support an uplift in maturity across sectors, including:

a. Introducing a more tailored, risk-based approach to supporting cyber maturity on a sector-by-sector basis, which should be accompanied by meaningful engagement mechanisms between the Government and relevant sectors;
b. Increasing collaboration among critical infrastructure and security regulators, which could be achieved through the establishment of a Cyber Regulators Forum.
c. Retaining CIRMP exemptions for data sector organisations with Strategic Hosting Certification to avoid regulatory duplication;
d. Clarifying intended scope of notifiable incident reporting obligations to ensure that availability incidents resulting from non-malicious technical failures are excluded from reporting;
e. Introducing separate forms for Part 2A and Part 2AA annual report obligations to improve clarity and guidance for SOCI Act reporting;
f. In keeping with the ambition for sector-by-sector approaches, consider extending the 30-day update requirement for the Asset Registry for the data sector;

g. Introduce a formal exemption mechanism from the Government Assistance Powers for entities with demonstrated cyber maturity, cooperative engagement history, and robust incident response capabilities. This would ensure the powers are applied proportionately and avoid unintended impacts on complex cloud environments.

3. Aligning obligations with international best practice

Businesses operating across borders face a growing patchwork of divergent cyber security regulations in different jurisdictions, from incident reporting rules to cloud security certifications. Inconsistent rules are driving up compliance costs, creating operational complexity, and diverting resources away from security improvements impacting overall resilience. For companies operating across multiple markets, navigating a patchwork of definitions, timelines, and reporting thresholds is not only inefficient but also risks undermining the effectiveness of incident response and coordination.

From a security standpoint, regulatory fragmentation can inadvertently hinder collective defence. For example, when incident reporting requirements vary widely between jurisdictions, it becomes harder to share timely, actionable intelligence across borders. This slows down the detection of systemic threats and weakens the global response to malicious cyber activity. The Australian Strategic Policy Institute (ASPI) has recognised this challenge across the Indo-Pacific region and argued for a greater focus on regulatory alignment to reduce red tape and strengthen regional resilience.[3]

In this context, we encourage Australia to use the SOCI Act to lead by example in promoting regulatory harmonisation and reciprocity. The SOCI Act already does this in one important way – by recognising a range of global cyber security standards under the CIRMP obligations – but there are other areas where the regime diverges from global norms.

Incident reporting is one practical area ripe for international alignment. This includes definitions of reportable incidents, reporting timelines, and reciprocal recognition of reporting obligations. Several jurisdictions, including the US (forthcoming CIRCIA rules), are converging on a 72-hour window for reporting significant cyber incidents, while the EU (through the Network and Information Systems Directive 2 (NIS2)) requires an "early warning" within 24 hours and an incident notification within 72 hours. The SOCI Act's current dual requirement – a notification in 12 hours for an incident with a "significant" impact, or a report in 72 hours for an incident with a "relevant" impact – is complex, relatively unique and can be onerous. Additionally, a 12-hour notification timeframe may be challenging to operationalise in practice. The first hours of incident response are typically focused on containment, with limited information available to support an accurate notification.

Consolidating this into a single reporting timeline of 72-hour, or a 24-hour early warning followed by a 72-hour notification for the "critical" incidents, would bring Australia in line with other key overseas regimes. It would also simplify the potential for mutual recognition of incident reports with allies so that a report filed to one jurisdiction can satisfy others, at least in part. Beyond timing, definitions of what must be reported, and thresholds for when reporting is required, should also be aligned internationally.

[3] ASPI 2025, Indo-Pacific needs alignment, not uniformity, to remove cyber red tape

By focusing on this foundational area, Australia can reduce regulatory friction, improve cross-border coordination, and help ensure that cybersecurity regulations support, not hinder, security outcomes.

Recommendation 3: Prioritise international regulatory alignment and interoperability, with an initial focus on incident reporting. This should include: i) aligning the 12-hour and 72-hour incident reporting window under the SOCI Act into a single 72-hour requirement, or a 24-hour early warning followed by a 72-hour notification for "critical" incidents; ii) harmonising definitions of what must be reported and thresholds for reporting with key allies such as the Five Eyes and EU; and iii) exploring the potential for mutual recognition of incident reporting so that a report filed to one jurisdiction can satisfy others.

4. Maintaining a proportionate compliance and enforcement regime

Effective regulation creates incentives for compliance and holds organisations accountable for lapses without creating a punitive atmosphere that discourages collaboration and cooperation. Microsoft urges the Review to ensure the SOCI Act's enforcement regime remains proportionate, fair, and geared toward improving security outcomes.

The SOCI Act in its current form already contains a range of enforcement tools, including civil penalty provisions (fines) and even some criminal offences for serious failures. In practice, enforcement has been light-touch to date – appropriately so, as government and industry have worked together to raise awareness of expectations and baseline compliance.

We note Australia is still relatively unique globally in having a penalty-backed critical infrastructure cyber law. This means Australia is at the forefront, and any move to further ratchet up penalties should be carefully evaluated against potential unintended negative consequences (such as a hesitance by responsible entities to report incidents or share information candidly with governments, and an outsized impact and potential chilling effect on local startup companies) which may act against the goals of the legislation to improve visibility of threats and drive greater collaboration to uplift the nation's resilience.

With that being said, having credible penalties and the willingness to use them in egregious cases is a necessary backstop to ensure compliance. We anticipate that as the SOCI regime matures, the regulator will take enforcement action against non-cooperative or persistently non-compliant entities, and rightly so. The key is to apply enforcement in a way that encourages better security. In this light, Microsoft suggests:

- Keeping the primary focus on civil enforcement and using criminal prosecution only as a very last resort for extreme, deliberate violations;
- Building in incentives for positive behaviour so organisations feel it's better to be open and proactive than to hide problems;
- Ensuring penalties remain proportionate and take account of the organisation's risk management practices;
- Continuing the current regulatory posture of engagement first, enforcement second to bring industry "along on the journey" to uplift resilience.

Recommendation 4: Preserve a proportionate approach to compliance and enforcement under the SOCI Act that seeks to incentivise positive behaviour and encourage cooperation.

Microsoft appreciates the opportunity to contribute these perspectives. We are committed to our continued partnership with the Australian Government to protect the cyber and national security of Australia and ensure the SOCI Act continues to achieve its objectives. We are available to discuss our observations and recommendations in greater detail at your discretion.

Sincerely,

[redacted]

[redacted]