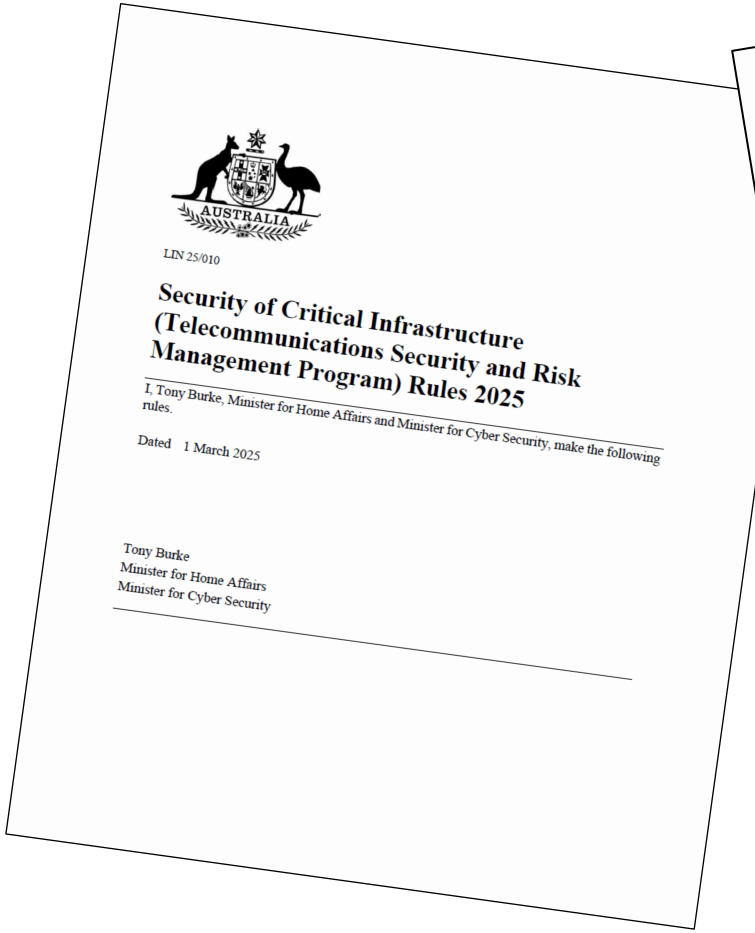


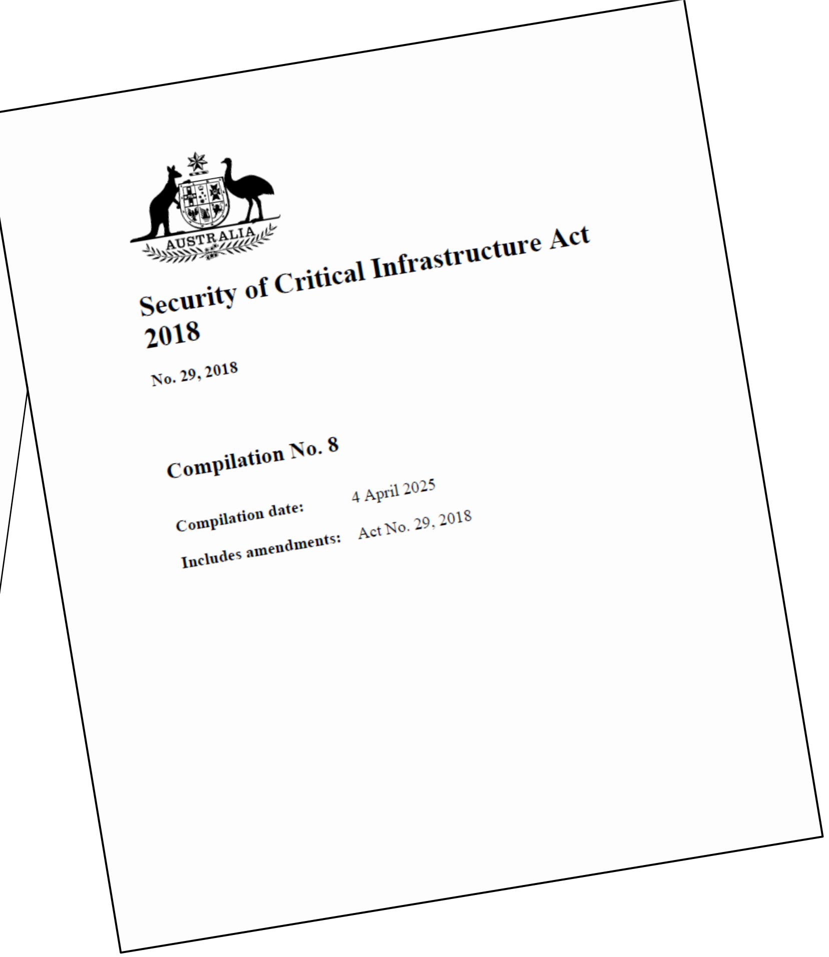
LIN 25/010

Security of Critical Infrastructure (Telecommunications Security and Risk Management Program) Rules 2025

I, Tony Burke, Minister for Home Affairs and Minister for Cyber Security, make the following rules.

Dated 1 March 2025

Tony Burke
Minister for Home Affairs
Minister for Cyber Security



Security of Critical Infrastructure Act 2018

No. 29, 2018

Compilation No. 8

Compilation date:	4 April 2025
Includes amendments:	Act No. 29, 2018

Risky Business!

New Risk Management Obligations for Telcos

Sophia Joo – Internet Association of Australia

SOCI Act and TSRMP Rules

Security of Critical Infrastructure (Telecommunications Security and Risk Management Program) Rules 2025 (TSRMP Rules)

- New legislation switching on risk management obligations

Security of Critical Infrastructure Act 2018 (SOCI Act)

- Amended to consolidate rules relating to security and critical infrastructure previously under telecommunications legislation

What are the consolidated rules?

‘Protect your asset’ obligation:

Protect your ***critical telecommunications assets*** *so far as it is reasonably practicable to do so, where there is a* ***material risk*** *of harms that will have* ***relevant impact***

(“Reasonably practicable” added as per industry feedback…yay!)

What are the consolidated rules?

Notification obligation:

Notify of changes or proposed changes to your telco services or systems ***where that change is likely to have a material adverse effect*** *on your capacity to* ***comply with the obligation to protect your asset****.*

Examples:

- Changing the location of your equipment/services
- Entering into an outsourcing arrangement
- Procuring “notifiable equipment”

Examples where there is likely **no material adverse effect**:

- Like-for-like replacement of equipment
- Day-to-day changes such as software updates

What are the TSRMP Rules?

bolded terms defined here

All-hazards Risk Management Program

- Identify operational context of each **critical telecommunications asset**
- Identify each hazard where there is a **material risk** the hazard could have a **relevant impact** on your asset
    - Physical security and natural
    - Cyber
    - Personnel
    - Supply Chain
    - Minimise or eliminate that material risk and
    - Mitigate the relevant impact of the hazard
- Board-approved Annual Report (from FY2026)

What are the TSRMP Rules?

Cyber and Information Hazards:

- Comply with **maturity level 1**– by 4 Oct 2026
- Comply with **maturity level 2**– by 4 Oct 2027

  comply, not become certified

- Suggested frameworks:
  - ISO/IEC 27001:2023
  - Essential Eight
  - NIST Framework
  - AESCSF
  - Cybersecurity Capability Maturity Model

Do they apply to me?

Obligation	Carriers	CSPs w/ 20,000+ SIOs CSPs that supply Cth govt	All other CSPs
Protect your asset	✓ As of 4 Apr 2025*	✓ As of 4 Apr 2025*	✘
Risk Management Program	✓ By 4 Oct 2025	✓ By 4 Oct 2025	✘
Cybersecurity Framework Compliance	✓ Level 1 maturity by 4 Oct 2026 ✓ Level 2 maturity by 4 Oct 2027	✓ Level 1 maturity by 4 Oct 2026	✘
Notification	✓ As of 4 Apr 2025*	✘ As of 4 Apr 2025	✘
Mandatory Cyber Incident Reporting	✓ As of 4 Apr 2025*	✓ As of 4 Apr 2025*	✘ No longer applies as of 4 Apr 2025
Asset Registration	✓ As of 4 Apr 2025*	✓ As of 4 Apr 2025*	✘ No longer applies as of 4 Apr 2025
Notifying data service providers	✓ Since 2022	✓ Since 2022	✓ Since 2022
Responding to serious incidents	✓ Since 2022	✓ Since 2022	✓ Since 2022

*= these obligations previously existed under telecommunications legislation

But this is all too hard!! >_<

IAA is partnering with the Wireless Internet Service Providers Association of Australia (**WISPAU**) to run group training sessions:

- Mastering the *SOCI Act*
- How to establish a Critical Infrastructure Risk Management Program
- Maximising Cyber Resilience
- How to conduct a security risk assessment

Cost-effective way to ensure compliance!

Please let us know if you’re interested!