Australian Government

Department of Home Affairs

Cyber Security Legislative Reforms – Explanatory Document

Security of Critical Infrastructure Rules

© Commonwealth of Australia 2024

With the exception of the Commonwealth Coat of Arms, all material presented in this publication is provided under a Creative Commons Attribution 4.0 International license at https://creativecommons.org/licenses/by/4.0/legalcode.

This means this license only applies to material as set out in this document.

The details of the relevant license conditions are available on the Creative Commons website at https://creativecommons.org/ as is the full legal code for the CC BY 4.0 license at https://creativecommons.org/licenses/by/4.0/legalcode.

Use of the Coat of Arms

The terms under which the Coat of Arms can be used are detailed at the Department of the Prime Minister and Cabinet website— https://www.pmc.gov.au/government/commonwealth-coat-arms.

Contact us

Enquiries regarding the licence and any use of this document are welcome at:

Department of Home Affairs

PO Box 25

BELCONNEN ACT 2616
P - 23-02503

Security of Critical Infrastructure Rules

Context

Threats to the operation of Australia's critical infrastructure continue to be significant and far-reaching. From natural hazards through to human-induced threats—all have the potential to significantly disrupt critical infrastructure. The *Security of Critical Infrastructure and Other Legislation Amendment (Enhanced Response and Prevention) Act 2024* (ERP Act) enhances the security and resilience of critical infrastructure in the face of all hazards. New Rules and amendments to existing Rules will support implementation of the ERP Act. This explanatory document accompanies the start of formal consultation on the Rules, which closes on 13 February 2025.

The Department will continue to work alongside industry to streamline implementation and promote a shared understanding of security and resilience.

Part 1 – Telecommunications security and risk management program

Background

The Draft *Security of Critical Infrastructure (Telecommunications Security and Risk Management Program) Rules 2024* (Draft TSRMP) are a new instrument, to be made by the Minister of Home Affairs under Part 2A (critical infrastructure risk management programs) and Part 2D (security regulation for critical telecommunications assets) of the SOCI Act. The TSRMP Rules proportionately apply and clarify security obligations for critical telecommunications assets under the SOCI Act. The Draft TSRMP reflects a lengthy process of co-design through the Australian Telecommunications Security Reference Group.

The explanatory document clarifies the interpretation of the draft TSRMP at key points, including on how the risk management program obligations and material risk are intended to function. The TSRMP, once made, will be accompanied by detailed guidance material that creates a consistent, industry-wide approach to telecommunications security.

The Department maintains its intention to allow entities to group assets for the purposes of reporting on and complying with Part 2A requirements. Subsection 4(4) of the *Security of Critical Infrastructure (Critical infrastructure risk management program) Amendment (Data Storage Systems) Rules 2024* establishes this mechanism beyond legal doubt.

Proportionate obligation application

Sections 4 and 5 together create a mechanism to proportionately apply security obligations in Parts 2A and 2D of the SOCI Act to asset types of varying size and criticality. The mechanism preserves the broad capture of all critical telecommunications assets in the SOCI Act for the purposes of Government assistance, information gathering and directions powers while limiting positive security obligations to a smaller subset of critical telecommunications assets.

The threshold balances security outcomes with regulatory burden and allows flexible collaboration between government and industry as the security and threat environment evolves. As detailed further below under “Application Rules”, this threshold is also intended to apply to obligations under the existing Part 2 (register of critical infrastructure assets) and Part 2B (mandatory cyber incident reporting – MCIR).

The Draft TSRMP applies key obligations to the assets of all carriers and a subset of carriage service providers that meet the prescribed threshold of 20,000 active carriage services or supply to the Commonwealth (except for bodies established by a law of the Commonwealth). The threshold is applied only to carriage service providers because of the security criticality and interrelatedness of carrier’s infrastructure. However, feedback received through informal consultation on the draft TSRMP suggested that a scope out mechanism could be established for entities who hold a carrier licence but are identified to not be security critical.

The Department, through the consultation period, welcomes early engagement and submissions from entities or peak bodies on the form that the exemption mechanism for carriers could take and which entities should be considered for this.

The threshold applies powers and obligations under the SOCI Act according to the following table:

	Notify data service providers s. 12F(3)	Asset Register Part 2	MCIR Part 2B	Obligation to protect asset, including risk management program Parts 2A and 2D	Notification obligation Part 2D	ECSOs for declared systems of national significance Part 2C	Government assistance; directions & information gathering power Parts 2D, 3, 3A, & 4
Carrier's assets	✓	✓	✓	✓	✓	May apply	✓
Relevant CSP asset (meet threshold)	✓	✓	✓	✓			✓
Critical telecommunications assets that do not meet threshold	✓						✓

Relevant carriage service provider asset

The TSRMP defines *relevant carriage service provider assets* as a subset of in-scope carriage service provider assets for the risk management program obligation (Part 2A). The intent is for captured carriage service providers to comply with the obligations above when they provide 20,000 or more active carriage services or supply to government or defence. The Department intends for the scope of carriage services to be captured as follows:

- Broadband services, which includes services connected by means of a:
    - fibre to the Building connection;
    - fibre to the Curb connection;
    - fibre to the Node connection;
    - fibre to the Premises connection;
    - fixed wireless internet connection;
    - hybrid Fibre Coaxial connection;
    - fixed line services;
    - satellite connection;
    - any other connection type;
- fixed telephone services;
- public mobile telecommunications services;
- voice only services.

The Department intends for the responsible entity for an asset that meets the definition to comply with the positive security obligations to:

- Protect the critical telecommunications asset (including by complying with risk management obligations under Part 2A of the Act)
- Comply with MCIR requirements (Part 2B of the Act);
- Provide information to the register of critical infrastructure assets (Part 2 of the Act).

Compliance grace period

Section 7 of the TSRMP establishes a compliance grace period for relevant CI assets required to comply with the Part 2A CIRMP obligations. Obligations to comply with the risk management program and associated reporting obligations will not commence until 6 months after the instrument commences, or 6 months after the asset becomes a relevant CI asset. As described below, further compliance grace periods exist for compliance with cyber security frameworks.

Guidance material

The Department, alongside the ATSRG and other agencies, will produce guidance material to support education and compliance with the TSRMP Rules. This guidance material will integrate and update existing material, including the Guidance for the Critical Infrastructure Risk Management Program and the Telecommunications Sector Security Reforms (TSSR) Administrative Guidelines (TSSR Guidance). The guidance material will include:

- key implementation timeframes (such as grace periods and reporting obligations);
- examples demonstrating the scope of the TSRMP;
- examples of when a responsible entity should notify of changes, including types of changes;
- explanations of key terms and all material risks and hazard domains; and
- further guidance as requested by government and industry.

Requirement for a responsible entity to protect their critical telecommunications asset

The TSRMP Rules largely mirror the existing *Security of Critical Infrastructure (Critical infrastructure risk management program) Rules (LIN 23/006) 2023* (CIRMP Rules) with additions to reflect telecommunications-specific risks and to provide further information on compliance with the obligation to notify certain changes and proposed changes to telecommunications service or system (section 30EC of the Act). While section 30EB(3)(c) states that an entity must comply with any other requirements prescribed by the rules, the Department does not intend to prescribe additional requirements at this time.

The critical infrastructure risk management program

The TSRMP provides a version of the CIRMP obligations, with additional security obligations, that are tailored to suit the telecommunications sector. As such, it is the intent that the TSRMP could be considered as a subset of the broader CIRMP obligations, preserving interactions with other legislative frameworks, such as the AusCheck Act 2007.

Some concepts defined and introduced in the SOCI Act are crucial to compliance with the CIRMP in the Draft TSRMP Rules, though this may not be apparent on the face of the Rules. Guidance will clarify.

Material risk

Material risks are defined by the TSRMP Rules to include a variety of risks that could have a *relevant impact on* a relevant CI asset if they occurred. Paragraph 30AH(1)(b) of the Act requires an entity to identify, minimise, or eliminate material risks to assets to the extent that they threaten to have a *relevant impact* on the asset. *Relevant impact* is defined by section 8G of the Act to mean a hazard that impacts on the availability, integrity, or reliability or confidentiality of the asset. In effect, while the material risks in the Draft TSRMP could be read as unrestrained in isolation, they are limited by the harms set out in section 8G of the Act.

Material risks under the TSRMP Rules include:

- a stoppage or major slowdown of the critical asset's function for an unmanageable period;
- an impairment of the critical asset's functions that prejudices the social or economic stability, or defence or national security, of Australia;
- a substantive loss of access to, or deliberate or accidental manipulation of, a critical component of the critical asset;
- an interference with the critical asset's operational or information communication technology essential to the functioning of the asset;
- the storage, transmission or processing of sensitive operational information outside Australia;
- remote access to operational control or operational monitoring systems of the CI asset;
- compromise, theft or manipulation of communications;

- unauthorised access to or unauthorised use of a critical asset by a:
    - major supplier; or
    - critical worker; or
    - managed service provider;
- risks to data storage systems that hold business critical data, where vulnerabilities could impact the availability, integrity, reliability or confidentiality of the asset.

This broadly replicates the material risks captured within the CIRMP Rules, with some amendments to reflect material risks unique to critical telecommunications assets. As discussed above, material risks should be minimised, mitigated or eliminated, so far as it is reasonably practicable to do so, to the extent that they could have an impact on the availability, integrity, or reliability or confidentiality of the asset.

A practical example may include risks generated from remote offshore network access to the extent that those risks could cause an incident which results in carriage services becoming unavailable to end-users. Similarly, a stoppage or major slowdown of the asset would only meet the *relevant impact* threshold if it were to significantly affect the usability of the network for customers and end-users. Terms such as 'unmanageable period' are not dictated by government, as entities are best placed to determine the magnitude of impacts to their asset, but guidance will support industry to make those decisions.

General – all hazards

Section 9 - 'General – all hazards' of the Draft TSRMP Rules mirrors the existing CIRMP Rules. This section requires the responsible entity for a relevant CI asset to identify all material risks to their asset across 'all hazards' and to minimise or eliminate those risks so far as it is reasonably practicable to do so. Section 9 establishes the conditions that an entity's written risk management program must satisfy, including that it:

- is reviewed and up to date;
- identifies and provides contact details for each position within the entity that is responsible for developing, implementing and complying with the risk management program;
- contains a risk management methodology; and
- describes how the risk management program will be reviewed.

Cyber and information security hazards

Section 10 of the TSRMP Rules requires responsible entities to minimise or eliminate any material risk of a cyber and information security hazard from occurring and mitigate the relevant impact of a cyber and information hazard on the asset. This section is one of the more complex sections within the Draft TSRMP and will be accompanied by detailed guidance to assist compliance. Section 10's main function is to prescribe minimum cyber security maturity frameworks for entities to meet within prescribed time periods.

All entities responsible for a relevant CI asset will be required by section 10 to establish and maintain a process or system to meet, where relevant, at least maturity indicator 1 in one of the cyber security frameworks listed in the TSRMP Rules or an equivalent framework. The entity would be required to meet this condition within 12 months after the end of the 6-month grace period. For the responsible entity for a relevant carriage service provider asset, no further standard will need to be met at this time. This will form the baseline for all in scope critical telecommunications assets and is commensurate with all entities who comply with the CIRMP.

Responsible entities for carrier owned or operated assets would additionally need to meet maturity indicator 2 of the relevant frameworks within 12 months of meeting maturity indicator 1. This is because the Department, in close consultation with government agencies and industry through the ATSRG, has determined that it would be appropriate for a subset of critical telecommunications assets to maintain a higher cyber baseline than other critical infrastructure assets. This responds to the heightened risk environment for critical telecommunications assets and their centrality to the security and prosperity of Australians.

The maturities and milestones of section 10 are laid out in the table below:

	Compliance Period After Switch-on of the Rules (or when the asset later becomes a critical telecommunications asset)		
	6 months	18 months	30 months
Carrier's assets	**TSRMP**	**Cyber Framework – Maturity indicator 1**	**Cyber Framework – Maturity indicator 2**

Carriage service provider's assets **(that meet threshold)**	**TSRMP**	**Cyber Framework – Maturity indicator 1**	**Maintain MI1 and update according to threat environment**

Because some cyber security frameworks do not contain maturity indicator levels, the TSRMP Rules allow an entity to comply with their preferred cyber security framework where they document, in their written risk management program, the steps taken to make their program equivalent to maturity indicator 2 of an appropriate cyber maturity framework. This measure requires entities to demonstrate that, where no maturity indicator is built into the framework, such as the *Framework for Improving Critical Infrastructure Cybersecurity* published by the National Institute of Standards and Technology of the United States of America (NIST framework), that their use of the framework is equivalent to maturity indicator 2. The NIST framework has been highlighted as a preferred cyber maturity framework during industry consultation due to its international application and operating system-agnostic approach.

The Department will work with industry to produce guidance on how such equivalence might be documented to ensure a consistent approach to cyber security is adopted across telecommunications assets.

Personnel hazards

Section 11 of the Draft TSRMP describes 'personnel hazards'. These require a responsible entity to establish and maintain in their risk management program, as far as it is reasonably practicable to do so, a system to minimise or eliminate material risks relating to malicious or negligent personnel. A responsible entity must identify critical workers and assess their suitability to access critical components of the asset. Entities may choose to engage the AusCheck background check scheme to conduct this suitability assessment.

An AusCheck check allows entities to conduct a background check that includes:

- identity verification;
- a criminal record assessment against CIRMP security relevant offences by AusCheck using information collected by the Australian Criminal Intelligence Commission (ACIC);
- a national security assessment by the Australian Security Intelligence Organisation (ASIO);
- a 'right to work in Australia' check if a person is not an Australian citizen, conducted through the Visa Entitlement Verification Online (VEVO) system.

Entities are not compelled to use the AusCheck scheme and may choose how they comply with the suitability assessment requirement.

Supply chain hazards

Section 12 of the Draft TSRMP contains supply chain hazards and requires a responsible entity to address vulnerabilities in the supply chain, including the following material risks:

- unauthorised access, interference or exploitation of the asset's supply chain; and
- misuse of privileged access to the asset by any provider in the supply chain; and
- disruption of the asset due to an issue in the supply chain; and
- arising from threats to people, assets, equipment, products, services, distribution and intellectual property within supply chains; and
- arising from major suppliers; and
- any failure or lowered capacity of other assets and entities in the entity's supply chain; and
- as far as it is reasonably practicable to do so, mitigate the relevant impact of a supply chain hazard on the asset.

Physical security and natural hazards

Section 13 of the Draft TSRMP contains 'physical security and natural hazards' and requires a responsible entity to establish and maintain in their risk management program a process or system:

- to identify the physical critical components of the CI asset; and
- to control access to physical critical components; and
- for responding to incidents where unauthorised access to a physical critical component occurs; and

- for managing and mitigating a variety of physical security hazards and natural hazards to their CI assets; and
- to test that security arrangements are effective and appropriate and promote resilience.

Responsible entity's notification obligations

Section 14 of the Draft TSRMP clarifies the information relevant to an entity's circumstances that they should provide to the Secretary under the section 30EC requirement to notify of certain changes and proposed changes to telecommunications service or system. Section 14 promotes a flexible system, driven by the principle of providing sufficient information to allow the Secretary to collaborate with industry and offer pertinent risk advice.

Section 14 enhances clarity for a responsible entity on what is expected of them to protect national security interests and promotes transparency and accountability. Government and industry anticipate that this would encourage engagement with government agencies on managing security risks such as espionage, sabotage and foreign interference and speed up the assessment process.

Where reasonably practicable to produce and relevant to the context of the change or proposed change, section 14 requires a responsible entity's notification to contain information about the change or proposed change, including:

- a security risk assessment;
- information about relevant controls for identified risks;
- descriptions of hardware and software being introduced;
- details about major suppliers for the project;
- schematics and system documentation;
- a timeline of the proposed change;
- any other relevant information.

Part 2 – Amendments to the Application Rules

Summary of changes

Some critical telecommunications assets are currently subject to 'SOCI-like' obligations applied under the Telecommunications Act, namely the Asset Register and MCIR obligations, through the *Telecommunications (Carrier License Conditions—Security Information) Declaration 2022* and the *Telecommunications (Carriage Service Provider—Security Information) Determination 2022*. These instruments will be repealed.

The *Security of Critical Infrastructure (Application) Rules (LIN 22/026) 2022* is being amended be amended to apply these obligations to a subset of critical telecommunications assets. This subset mirrors the assets captured by the TSRMP Rules, i.e. all carrier assets and 'relevant carriage service provider assets', as per the above heading 'Relevant carriage service provider threshold'.

Part 3 – Amendments to the Critical Infrastructure Risk Management Program Rules

Schedule 1 of the ERP Act amends the SOCI Act definition of 'critical infrastructure asset' to specify that data storage systems that store or process business critical data are part of the critical infrastructure asset, where vulnerabilities in those systems could impact the function of that asset.

Schedule 1 clarifies the application of obligations for critical infrastructure assets under the SOCI Act, including the CIRMP obligation, to those data storage systems. Under the amendments, critical infrastructure entities currently captured by the SOCI Act will be explicitly required to identify and control against risks to their data storage assets as part of their CIRMP. This would require the responsible entity to identify material risks to data storage systems holding 'business critical data' and minimise or eliminate those risks across 'all hazards', including cyber, personnel, supply chain, physical security and natural hazards.

/