EXPLANATORY STATEMENT

Issued by authority of the Minister for Home Affairs and the Minister for Cyber Security

Security of Critical Infrastructure Act 2018

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

Legislative Authority

The *Security of Critical Infrastructure (Telecommunications Security and Risk Management Program) Rules 2025* (the TSRMP Rules), are made under section 61 of the *Security of Critical Infrastructure Act 2018* (the SOCI Act). This provision allows the Minister to make, by legislative instrument, rules prescribing matters required or permitted by the SOCI Act, or that are necessary or convenient to be prescribed for carrying out or giving effect to the SOCI Act.

This instrument is an establishing instrument, which introduces a new set of Rules given authority by the SOCI Act. Subsection 33(3) of the *Acts Interpretation Act 1901* states that a power to make a legislative instrument includes a power to repeal, rescind, revoke, amend, or vary that instrument in the same manner, and subject to the same conditions, as the power to make the instrument.

Purpose and background

The *Security of Critical Infrastructure and Other Legislation Amendment (Enhanced Response and Prevention) Act 2024* (the ERP Act) amended the SOCI Act to give effect to the legislative reforms outlined under Shield 4 of the *2023-2030 Australian Cyber Security Strategy* and subsequent *2023-2030 Australian Cyber Security Strategy: Cyber Security Legislative Reforms Consultation Paper*.

Schedule 5 of the ERP Act amended the SOCI Act to incorporate elements of the Telecommunications Sector Security Reforms, administered by the Home Affairs portfolio. These amendments included security and notification obligations from Part 14 of the *Telecommunications Act 1997* (Telecommunications Act), with enhancements to align the regulatory frameworks and clarify telecommunications-specific obligations.

The TSRMP Rules complement the amendments made by the ERP Act and provide a proportionate framework of security obligations specifically tailored to critical telecommunications assets and the unique hazards that may affect telecommunications assets which may be addressed through a telecommunications-specific Critical Infrastructure Risk Management Program (CIRMP).

The TSRMP Rules operationalise Part 2A of the SOCI Act for relevant critical infrastructure assets, which are a subset of critical telecommunications assets, by prescribing requirements for a telecommunications sector-specific CIRMP (TSRMP) The TSRMP Rules also enliven the enhanced security regulations contained in Part 2D of the SOCI Act for relevant critical infrastructure assets. Parts 2A and 2D were inserted into the SOCI Act by the ERP Act and will commence on a day to be fixed by Proclamation.

Section 5 of the TSRMP Rules defines a ‘relevant critical infrastructure asset’ as a critical telecommunications asset that is owned or operated by a carrier or a relevant carriage service provider asset This definition seeks to adopt a proportionate threshold-based approach by targeting a narrower class of critical telecommunications assets for the imposition of positive security

Authorised Version Explanatory Statement registered 11/03/2025 to F2025L00325

obligations in the SOCI Act while preserving the application of government assistance, information gathering and directions powers for all critical telecommunications assets.

See discussion in '**Attachment A'** for further guidance on the definitions of a 'relevant critical infrastructure asset' and 'relevant carriage service provider asset'.

Enlivening Part 2A of the SOCI Act for relevant critical infrastructure assets

Section 7 of the TSRMP Rules specifies particular critical infrastructure assets to which Part 2A of the SOCI Act applies, as required by paragraph 30AB(1)(a) of the SOCI Act. Section 7 additionally provides for a compliance grace period, which suspends application of Part 2A for relevant critical infrastructure assets until the later of 6 months after the commencement of the TSRMP Rules, or 6 months after the asset becomes a relevant critical infrastructure asset.

Part 2A of the SOCI Act imposes CIRMP obligations, as operationalised for other specified critical infrastructure assets by the existing instrument, the *Security of Critical Infrastructure (Critical infrastructure risk management program) Rules (LIN 23/006) 2023* (CIRMP Rules). The TSRMP obligations replicate and enhance the existing provisions within the CIRMP Rules, for specified assets for which responsible entities must comply with. This includes the obligation that responsible entities maintain a CIRMP, including additional telecommunications-specific requirements.

As specified in section 30AH(1) of the SOCI Act, a CIRMP is a written program:

a) that applies to a particular entity, which is the responsible entity for one or more critical infrastructure assets; and

b) that does the following for each of those assets:

   i) identifies each hazard where there is a material risk that the occurrence of the hazard could have a relevant impact on the asset;

   ii) so far as it is reasonably practicable to do so—minimises or eliminates any material risk of such a hazard occurring;

   iii) so far as it is reasonably practicable to do so—mitigates the relevant impact of such a hazard on the asset; and

c) that complies with such requirements (if any) as are specified in the Rules related to the SOCI Act.

To support the operation of section 30AH of the SOCI Act, section 8 of the TSRMP Rules provides for a telecommunications-specific definition of "material risk", which applies for the purpose of a TSRMP. The definition reflects the definition of material risk provided for in the CIRMP Rules with amendments to reflect the unique risk environment that telecommunication assets operate within.

Part 3 of the TSRMP Rules specifies additional obligations for a TSRMP under paragraph 30AH(1)(c) of the SOCI Act. These obligations mirror those imposed by the CIRMP Rules with additional requirements being outlined under each type of risk within the TSRMP Rules. The most significant addition is the increased cyber security framework compliance requirements.

Authorised Version Explanatory Statement registered 11/03/2025 to F2025L00325

The elements replicated (with additions) from the CIRMP Rules and reflected in the TSRMP Rules include the obligations to:

- identify all material risks to their asset across all hazards and minimise or eliminate those risks as far as it is reasonably practical to do so as part of their CIRMP obligations (section 8 of the TSRMP Rules);
- meet certain governance requirements (section 9 of the TSRMP Rules);
- 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 (section 11 of the TSRMP Rules);
- identify critical workers and assess their suitability to access critical components of the asset (section 12 and 13 of the TSRMP Rules);
- address vulnerabilities in the supply chain (section 14 of the TSRMP Rules);

Enlivening Part 2D of the SOCI Act for critical telecommunications assets

The TSRMP Rules also enliven Part 2D of the SOCI Act which was introduced through the ERP Act, which provides telecommunications-specific obligations, replicated from existing requirements in the Telecommunications Act, to be imposed on specified critical telecommunications assets.

Section 6 of the TSRMP Rules turns on the application of subsection 30EB(1) of the SOCI Act to relevant critical infrastructure assets. Section 30EB of the SOCI Act establishes a positive obligation on responsible entities of the relevant critical telecommunications assets to protect these assets.

Section 16 of the TSRMP Rules prescribes the application of subsection 30EC(1) of the SOCI Act to critical telecommunications assets owned or operated by a carrier. Section 30EC of the SOCI Act contains an obligation on responsible entities to notify the Secretary of the Department of certain changes or certain proposed changes to telecommunications services or systems. Section 17 of the TSRMP Rules sets out the notification requirements for responsible entities to comply with.

The TSRMP Rules commence, in accordance with section 2, on the later of the day after the registration of this instrument, or immediately after the commencement of Parts 1 and 2 of Schedule 5 to the ERP Act.

Consultation

The Department engaged industry stakeholders responsible for critical telecommunications assets during the development of the TSRMP Rules.

Before making this instrument the Minister, in accordance with section 30ABA of the SOCI Act:

a) published a notice on the Department's website:
   - setting out the draft rules made for the purposes of section 30ABA of the SOCI Act; and
   - invited persons to make submissions to the Minister about the draft rules within a period not shorter than 28 days (the notice specified a period of 60 days, commencing on 16 December 2024 and ending on 14 February 2025; and

b) provided a copy of the notice to each First Minister; and

Authorised Version Explanatory Statement registered 11/03/2025 to F2025L00325

c) considered all submissions received, which included 20 written submissions.

All submissions were reviewed and considered in the making of the TSRMP Rules. Minor changes were made as a result of the consultation process. These changes clarified the operation of section 11, which relates to cyber and information hazards. In particular, the Department has:

- amended the instrument to allow a relevant critical infrastructure asset to comply with an equivalent cyber security framework. This ensures entities can comply with the framework that best mitigates cyber security risks in their operating environment where that framework lacks maturity indicators.
- updated the title of the AS/NZS ISO/IEC 27001 document to reflect the latest version.

Beyond the formal consultation requirements in section 30ABA of the SOCI Act, the Department also hosted:

- a Town Hall on 16 December 2024, which provided an overview of the proposed Rules as well as what to expect during the consultation period to assist stakeholders to understand the changes and inform their feedback;
- a closed-door session for key affected stakeholders in the Australian Telecommunications Security Reference Group (ATSRG) on 21 January 2025;
- two public TSRMP Rules Deep Dive sessions on 30 January 2025 and 11 February 2025; and
- bilateral engagements with industry and peak bodies.

In these circumstances, the Minister was satisfied that appropriate consultation was undertaken, in accordance with section 17 of the *Legislation Act 2003* because:

- persons likely to be affected by the instrument had an adequate opportunity to comment on the draft instrument;
- the Department engaged stakeholders with targeted written communications to ensure responsible entities were aware of the proposed changes and could comment; and
- the instrument was co-designed with the ATSRG over a period of more than 6 months, drawing upon the knowledge and expertise of telecommunication industry stakeholders and peak bodies.

The Department of Home Affairs has previously certified a Regulatory Impact Statement for the *Security of Critical Infrastructure (Critical infrastructure risk management program) Rules (LIN 23/006) 2023* (the 2022 RIS). A summary of the findings of the 2022 RIS is below.

The *Supplementary Analysis for Critical Telecommunications assets* (Supplementary IA) (**Attachment C**) was prepared to supplement the impact analysis (IA) in the 2022 RIS and is to be relied upon for the purpose of the TSRMP Rules. The supplementary analysis was developed in consultation with the ATSRG.

The 2022 RIS analysed the economic impact of introducing the critical infrastructure risk management program for specified asset classes. The 2022 RIS conducted analysis relating to the economic impact of the critical infrastructure risk management program obligation as set out in both the SOCI Act and the CIRMP Rules.

The analysis in this RIS was the subject of considerable industry consultation and economic modelling based on industry cost estimates to conclude that the cost of introducing a mandatory RMP framework most effectively addressed the policy issues identified, offering the greatest net benefit of the policies considered.

Authorised Version Explanatory Statement registered 11/03/2025 to F2025L00325

The Supplementary IA weighs the regulatory costs of the measures against the damage to the economy if businesses underinvests in security and allow breaches to occur. The Supplementary IA clearly identifies that the regulatory costs of complying with the critical infrastructure risk management program obligation is minimal when compared to the damage to the economy if businesses underinvest in security and allow breaches to occur.

The Supplementary IA highlights that existing regulatory frameworks and market forces are insufficient to protect critical infrastructure against all hazard threats in a consistent and coordinated manner across critical telecommunication assets. Moreover, the likely benefits of the TSRMP obligation will be at least (and are expected to be more than) the costs of the regulation. This is primarily because the frequency and severity of all hazard risks for critical telecommunication assets are growing and this increasing severity and frequency of incidents, particularly in the context of growing cybersecurity incidents, represents a risk to the whole economy.

Economic analysis indicates that the potential cost of the required security uplift would be outweighed by the net benefits to the economy.

Other matters

The instrument is a legislative instrument for the purposes of the *Legislation Act 2003* and is subject to disallowance.

Details of the instrument are set out in **Attachment A**.

A Statement of Compatibility with Human Rights provides that the instrument is compatible with human rights because to the extent that it may limit human rights, those limitations are not arbitrary or unlawful and are reasonable, necessary and proportionate to pursue the legitimate objective of national security and public order. The Statement is included at **Attachment B**.

Authorised Version Explanatory Statement registered 11/03/2025 to F2025L00325

Attachment A

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

Part 1 Preliminary

Section 1 Name

Section 1 provides that the name of the instrument is the *Security of Critical Infrastructure (Telecommunications Security and Risk Management Program) Rules 2025* (the instrument).

Section 2 Commencement

Section 2 provides that the instrument commences on the later of:

a. The day after this instrument is registered; and

b. Immediately after the commencement of Parts 1 and 2 of Schedule 5 to *Security of Critical Infrastructure and Other Legislation Amendment (Enhanced Response and Prevention) Act 2024* (the ERP Act).

Commencement of this instrument is predicated on the commencement of Parts 1 and 2 of Schedule 5 of the ERP Act since these Parts give effect to the legislative frameworks on which this instrument is based. Parts 1 and 2 of Schedule 5 to the ERP Act are to commence on a day fixed by Proclamation.

Section 3 Authority

Section 3 provides that the instrument is made under section 61 of the *Security of Critical Infrastructure Act 2018* (the SOCI Act).

Subsection 33(3) of the *Acts Interpretation Act 1901* relevantly provides that a power to make a legislative instrument includes a power to repeal, rescind, revoke, amend, or vary that instrument in the same manner, and subject to the same conditions, as the power to make the instrument.

Section 4 Definitions

Section 4 sets out definitions of terms that are relied upon within the instrument.

The note under section 4 of the instrument provides that a number of expressions used in the instrument are defined in section 5 of the SOCI Act, including ***critical infrastructure asset*** and ***responsible entity***. For the purposes of this instrument the term ***Secretary*** is given the meaning in Section 5 of the SOCI Act, except, for the purposes of subsection 11, where ***Secretary*** is to have the same meaning as in subsection (4)(1) of the *AusCheck Act 2007* (AusCheck Act).

This section defines the following terms for the purpose of the instrument:

- ***Act*** means the SOCI Act.

Authorised Version Explanatory Statement registered 11/03/2025 to F2025L00325

- ***AusCheck Act*** means the *AusCheck Act 2007*.

- ***AusCheck Regulations*** means the *AusCheck Regulations 2017*.

  Background check is defined to have the same meaning as its definition in section 5 of the AusCheck Act.

- ***Broadband Services*** is defined to mean one or more services connected by means of a fibre to building connection, fibre to the curb connection, fibre to the premises connection, fixed wireless internet connection, hybrid fibre coaxial connection, fixed line services, satellite connection or any other connection type. This ensures that any physical or digital connection that transmits telecommunication information or services is accounted for in the instrument. The use of 'any other connection type' ensures the inclusion of any other technology that is not listed but that may provide broadband services. This ensures that all relevant connection types are captured for carriage service providers required to comply with the CIRMP obligations, particularly as technology evolves.

- ***CIRMP*** is defined to mean critical infrastructure risk management program.

- ***CIRMP criminal record*** has the same meaning as its definition in section 4 of the AusCheck Regulations.

- ***Communications*** is defined to have the same meaning as in the *Telecommunications Act 1997* (Telecommunications Act).

- ***Criminal history criteria*** is defined to mean the assessment of whether the person has a CIRMP criminal record and the nature of the offence.

- ***Cyber and information security hazard*** is defined to include where a person, whether authorised or not:

  (a) improperly accesses or misuses information or computer systems about, or related to, the relevant critical infrastructure asset; or
  (b) uses a computer system to obtain unauthorised control of, or access to, the relevant critical infrastructure asset, where that control or access may impair its proper functioning.

  An example of a cyber and information security hazard may include malware, where malicious software can be used to deny access, obtain information, gain control or disrupt systems, causing a relevant impact to an entity's critical infrastructure asset.

- ***Major supplier*** means any vendor that by nature of the product or service they offer, has significant influence over the security of a responsible entity's critical telecommunications asset. For example, a major supplier to a telecommunications company could supply core components of the system such as transmitters or end-to-end software. Major suppliers may also include network management services the responsible entity outsources to overseas third parties.

Authorised Version Explanatory Statement registered 11/03/2025 to F2025L00325

- ***Natural hazard*** includes fire, flood, cyclone, storm, heatwave, earthquake, tsunami, space weather or biological health hazard (such as a pandemic).

- ***Network-to-network interface*** is defined to mean the physical or virtual point of connection or interconnection between a critical telecommunications asset owned or operated by the responsible entity with another critical telecommunications asset, or a computer that is owned or operated by a separate entity or third party. This ensures the capture of all relevant connection interfaces and equipment between two or more critical infrastructure assets, noting that interdependencies between critical infrastructure assets affect the security of each asset. This is particularly important in the context of changes to networks, where one vulnerability could cause upstream and downstream risks to assets. .

- ***Personnel hazard*** is defined to include where a critical worker acts, through malice or negligence to compromise the proper functioning of the relevant critical infrastructure asset or causes significant damage to the relevant critical infrastructure asset.

- ***Physical security hazard*** is defined to include the unauthorised access to, interference with, or control of a relevant critical infrastructure asset, that could compromise the proper function or the asset or to cause significant damage to the asset. For example, issues-motivated individuals could gain access to an insufficiently secured mast antenna to cause damage to the network infrastructure housed there.

- ***Relevant carriage service provider*** is defined to mean a critical infrastructure asset owned or operated by a carriage service provider where:
  (a) the asset is used in connection with the supply of at least 20,000 active total carriage services including any of the following: broadband services; fixed telephone services: public mobile telecommunications services; or voice only services; or
  (b) the responsible entity for the asset is aware that the asset is used in connection with carriage services supplied to a Commonwealth entity (other than a body corporate established by a law of the Commonwealth).

  Examples of what may be captured under the relevant service provider definition include, but are not limited to:
  - a business who provides public mobile telecommunication services of more than 20 000 active total carriage services, using a major carrier's network to provide the service;
  - a business providing internet services to more than 20 000 customers, using the wholesale network of a carrier to provide the service; and,
  - a fixed telephone service provider has a contract with a Commonwealth agency to provide telecommunications services to the entity, but the supply of active total carriage services under the contract is less than 20 000;

- ***Relevant critical infrastructure asset*** is defined in section 5 of the instrument.

- ***Supply chain hazard*** is defined to include malicious people, both internal and external, exploiting, misusing, accessing or disrupting a supply chain and over reliance on particular suppliers.

Authorised Version Explanatory Statement registered 11/03/2025 to F2025L00325

Section 5 Meaning of *relevant critical infrastructure asset*

Section 5 defines what a relevant critical infrastructure asset is for the purposes of this instrument and the assets that are required to comply with the requirements of the instrument.

A relevant critical infrastructure asset is a critical telecommunications asset that is owned or operated by a carrier or a relevant carriage service provider asset. A critical telecommunications asset is defined in section 5 of the SOCI Act as:

> *(a) a telecommunications network that is:*
> *(i) owned or operated by a carrier or a carriage service provider; and*
> *(ii) used to supply a carriage service; or*
> (b) *any other asset that is:*
> *(i) owned or operated by a carrier or a carriage service provider; and*
> *(ii) used in connection with the supply of a carriage service.*

A carrier is defined in the Telecommunications Act as an entity that is the holder of a carrier license, which is granted under section 56 of the Telecommunications Act.

A relevant carriage service provider asset is defined in section 4 of the instrument.

The note within this section refers to changes made to the SOCI Act by the ERP Act. Specifically, the note draws the readers' attention to subsection 9(7) of the SOCI Act, and provides that a data storage system is taken to be part of a critical infrastructure asset specified in this section if it:

- is owned or operated by the responsible entity for a critical infrastructure asset;
- is used, or to be used, in connection with the critical infrastructure asset;
- stores or processes business critical data;
- presents a material risk of a relevant impact on the critical infrastructure asset and there is a material risk that the occurrence of such a hazard could have an impact on the data storage system.

The note clarifies that the effect of subsection 9(7) of the SOCI Act is that obligations under Part 2A, in relation to a critical infrastructure asset specified in section 5 will also need to take into account the data storage system, if the data storage system satisfies the requirements under subsection 9(7) of the SOCI Act.

Part 2 Responsible entity's obligation to protect critical telecommunications assets

Section 6 Application of section 30EB of the Act

Section 6 is an application provision, which enlivens the requirements contained in Part 2D, Division 2 of the SOCI Act for responsible entities of particular critical telecommunications assets. Under subsection 30EB(1) of the SOCI Act, a responsible entity for a critical telecommunications asset

Authorised Version Explanatory Statement registered 11/03/2025 to F2025L00325

must comply with the additional obligations in Part 2D, Division 2 if the critical telecommunications asset is prescribed in rules for that purpose.

The purpose of this section is to require responsible entities for relevant critical infrastructure assets (which is defined in section 5 of the instrument) to, as far as it is reasonably practicable to do so, protect the asset to ensure:

a. the confidentiality of communications (as defined within the Telecommunications Act); and

b. the availability and integrity of the asset.

Compliance with the obligation outlined above to protect critical telecommunications assets includes compliance with any requirements that apply to the entity and the asset under Part 2A (CIRMP requirements) and the requirement to maintain competent supervision of, and effective control over, the asset. The Part 2A requirements are contained within Part 3 of the instrument.

Authorised Version Explanatory Statement registered 11/03/2025 to F2025L00325

Part 3 Critical infrastructure risk management programs requirements

Section 7 Application of Part 2A of the Act

Section 7 is an application provision for Part 3 of the Rules. This section enlivens the requirements in Part 2A of the SOCI Act relating to CIRMPs. Under Part 2A of the SOCI Act, CIRMP requirements apply to a critical infrastructure asset if the asset is specified in rules.

If CIRMP requirements are enlivened for particular critical infrastructure assets, the responsible entity for the critical infrastructure asset must have, and comply with, the CIRMP. A CIRMP is a document that specifies each hazard and, where there is a material risk of the hazard having a relevant impact on the asset, outlines measures to mitigate or reduce the material risk or relevant impact of the hazard eventuating.

Subsection 7(1) specifies, for the purpose of paragraph 30AB(1)(a) of the SOCI Act, that a relevant critical infrastructure asset is specified. For this purpose, a relevant critical infrastructure asset is defined in section 5 of the Rules.

The effect of subsection 7(1) is to turn on the requirements of Part 2A of the SOCI Act for responsible entities of critical telecommunications assets that are owned or operated by a carrier, or a relevant carriage service provider (relevant critical infrastructure assets). Responsible entities of those assets must have, and comply with, a CIRMP after commencement (subject to subsection 7(2)).

Subsection 7(2) prescribes, for the purpose of subsection 30AB(3) of the Act, when a relevant critical infrastructure asset becomes a critical infrastructure asset for the purpose of enlivening CIRMP requirements in Part 2A of the SOCI Act.

Subsection 7(2) specifies that requirements in Part 2A of the SOCI Act do not apply to responsible entities for relevant critical infrastructure assets until the later of 6 months after this instrument commences, or 6 months after the asset becomes a relevant critical infrastructure asset.

For assets that meet the definition of relevant critical infrastructure asset when this instrument commences, CIRMP obligations will apply to those assets 6 months after commencement. For assets that will become relevant critical infrastructure assets after commencement (e.g. new critical telecommunications assets), Part 2A requirements will not apply until 6 months after that asset first becomes a relevant critical infrastructure asset.

This provision will ensure that responsible entities for relevant critical infrastructure assets will have, regardless if it is a new or existing asset, 6 months to establish a CIRMP before Part 2A requirements apply.

Section 8 Material Risk

Section 8 specifies material risks that are required to be considered as part of a CIRMP for relevant critical infrastructure assets. The material risks outlined in this instrument replicate, with

Authorised Version Explanatory Statement registered 11/03/2025 to F2025L00325

amendments, the material risks captured within the CIRMP Rules, with some amendments to reflect material risks unique to critical telecommunications assets.

Section 8 of the instrument specifies what a material risk is in relation to a relevant critical infrastructure asset's CIRMP, for the purpose of subsection 30AH(8) of the SOCI Act. Subsection 30AH(8) allows rules to provide that a specified risk is taken to be a material risk for the purpose of section 30AH. Paragraph 30AH(1)(b) of the SOCI Act requires responsible entities 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 SOCI 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 TSRMP Rules could be read as unrestrained in isolation, they are limited by section 8G of the SOCI Act.

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 materially affect the usability of the network for customers and end-users.

The instrument specifies the following as material risks in relation to relevant critical infrastructure assets for this purpose:

- a stoppage or major slowdown of the relevant critical infrastructure asset's function for an unmanageable period (paragraph (a));

- an impairment of the relevant critical infrastructure asset's functions that prejudices the social or economic stability, or national security, of Australia (paragraph (b));

- a substantive loss of access to, or deliberate or accidental manipulation of, a critical component of the relevant critical infrastructure asset (paragraph (c)).

The example under paragraph (c) provides that the substantive loss of access to, or deliberate or accidental manipulation of, a critical component of the relevant critical infrastructure asset include the position, navigation and timing systems (PNT systems) affecting provision of service or function of the asset. PNT systems are crucial for the precise timing signals they provide which are necessary to operate telecommunications networks.

- interference with the relevant critical infrastructure asset's operational or information communications technology essential to the function of the asset (paragraph (d)).

The example under paragraph (d) provides that an interference with the relevant critical infrastructure asset's operational or information communications technology essential to the function of the asset includes a billing and charging system. Billing and charging systems permit real time charging based on network use, accrediting end-users and allowing access to carriage services.

Authorised Version Explanatory Statement registered 11/03/2025 to F2025L00325

- the storage, transmission or processing of information relevant to the operation of the relevant critical infrastructure asset outside of Australia (paragraph (e)). The subparagraphs in paragraph (e) provide a non-exhaustive list of relevant information for this material risk:
    - layout diagrams;
    - schematics;
    - geospatial information;
    - configuration information;
    - operational constraints or tolerances information; or
    - data that a reasonable person would consider to be confidential; or sensitive about the asset
- remote access to operational control or operational monitoring systems of the relevant critical infrastructure asset (paragraph (f));
- compromise, theft or manipulation of communications (paragraph (g));
- unauthorised use which compromises the security and function of a relevant critical infrastructure asset (paragraph (h)). The subparagraphs in paragraph (h) provide a non-exhaustive list of who may gain authorised access for the purpose of this material risk and includes a major supplier, critical worker or managed service provider. The example under this paragraph provides that an example of this material risk is software installed by a major supplier on a modem without the knowledge of the responsible entity.
- impact on the availability, integrity, reliability or confidentiality of the data storage system holding business critical data (paragraph (i)).

In accordance with paragraph 30AH(1)(b) of the SOCI Act, the material risks identified must be considered by the responsible entity for a relevant critical infrastructure asset within their CIRMP to:

- identify hazards where there is a material risk (i.e. one of the risks outlined above) that could have a relevant impact on the asset if it occurred (subparagraph 30AH(1)(b)(i) of the SOCI Act); and
- establish and maintain a process or system in a CIRMP to—as far as it is reasonably practicable to do so—minimise or eliminate the material risks of such a hazard occurring (subparagraph 30AH(1)(b)(ii) of the SOCI Act).

Responsible entities must do this in relation to all hazards—including those specified in the instrument (e.g. personnel hazards) and any other hazard identified by the responsible entity that may adversely impact the asset. The purpose of section 8 is to specify certain ‘material risks’ for subsection 30AH(8) of the SOCI Act that a CIRMP must address with respect to those hazards. This list is non-exhaustive and an entity should seek to identify additional material risks that may apply across all-hazard domains.

Authorised Version Explanatory Statement registered 11/03/2025 to F2025L00325

For example, paragraph 8(e) of the instrument specifies that 'the storage, transmission or processing of information relevant to the relevant critical infrastructure asset outside of Australia' is a material risk. The failure for a CIRMP to minimise or eliminate material risks may lead to the occurrence of hazards that have a relevant impact on a critical infrastructure asset (as defined in section 8G of the SOCI Act) and specified further in this Part for relevant critical infrastructure assets.

Section 9 General requirements for a CIRMP

Section 9 of the instrument specifies the requirements that responsible entities for relevant critical infrastructure assets must ensure are contained in the CIRMP.

Subsection 9(1) of the instrument specifies, for paragraph 30AH(1)(c) of the SOCI Act, the general requirements a CIRMP for a relevant critical infrastructure asset must include in order to be compliant with section 30AH of the SOCI Act. For this purpose, subsection 9(1) prescribes that CIRMPs for relevant critical infrastructure assets must:

- identify the operational context of the relevant critical infrastructure asset (paragraph (a));
- identify the material risks to the relevant critical infrastructure asset (paragraph (b)), which may include those in section 8 of this instrument;
- as far as it is reasonably practicable to do so:
    - minimise or eliminate the material risks, including but not limited to the material risks specified in in section 8 of this instrument (subparagraph (c)(i)); and
    - mitigate the relevant impact of each hazard on the relevant critical infrastructure asset (subparagraph (c)(ii));
- include a mechanism to review the CIRMP to ensure compliance with section 30AE of the SOCI Act (paragraph (d)); and
- includes a mechanism to maintain the currency of the CIRMP to ensure it complies with section 30AF of the SOCI Act (paragraph (e)).

Section 9 specifies the general requirements for what a CIRMPs for relevant critical infrastructure assets must include, and includes hazards not specifically identified in the instrument.

Section 10 Adopting a CIRMP

Section 10 of the instrument specifies the requirements a responsible entity for a relevant critical infrastructure asset must have regard to in deciding to adopt a CIRMP.

Subsection 10(1) of the instrument prescribes, for subsections 30AKA(1) of the Act, matters a responsible entity must have regard to in deciding to adopt, review or vary a CIRMP. These are whether the CIRMP:

Authorised Version Explanatory Statement registered 11/03/2025 to F2025L00325

- describes the outcome of the process or system mentioned in paragraph 9(1)(a) (paragraph (a));
- describes interdependencies between each of the entity's relevant critical infrastructure assets and other relevant critical infrastructure assets (paragraph (b));
- identifies each position within the entity (paragraph (c)):
    - that is responsible for developing and implementing the CIRMP (subparagraph (c)(i)); and
    - for the processes mentioned in paragraph 9(1)(d)—that is responsible for reviewing the program or keeping the program up to date (subparagraph (c)(ii));
- contains the contact details for the positions covered by paragraph 10(1)(c) (paragraph (d));
- contains a risk management methodology (paragraph (e)); and
- describes the circumstances in which the entity will review the program (paragraph (f)).

The purpose of section 10 is to ensure that should a responsible entity for a relevant critical infrastructure asset adopt an existing CIRMP, they must have regard to the factors in subsection 10(1) to ensure the adopted CIRMP adequately addresses each matter specific to its operations. This will require, for example, the responsible entity to consider how the CIRMP will function on a daily basis, the kinds of relevant impacts and hazards that are most applicable to the assets, interaction with other critical infrastructure assets across and within sectors, and an overview of the process of risk management methodology that the CIRMP uses.

Section 11 Cyber and information security hazards

Section 11 specifies the cyber and information security hazard requirements that a responsible entity's CIRMP must comply with for the purposes of section 30AH(1)(c) of the SOCI Act.

The purpose of this section is to prescribe minimum cyber security requirements that responsible entities must comply with in their CIRMP for the purpose of addressing cyber and information security hazards.

Subsection 11(1) provides that subsections (2), (3) and (4) specify requirements, for paragraph 30AH(1)(c) of the SOCI Act.

Subsection 11(2) specifies that a CIRMP for a relevant critical infrastructure asset must include a process or system that, as far as it is reasonably practicable to do so, would:

- minimise or eliminate any material risk of a cyber and information security hazard occurring (paragraph 11(2)(a)); and

Authorised Version Explanatory Statement registered 11/03/2025 to F2025L00325

- mitigate the relevant impact of any cyber or information security hazard on the relevant critical infrastructure asset (paragraph 11(2)(b)).

The purpose of subsection 11(2) is to require a CIRMP for a relevant critical infrastructure asset to include a process or system that is sufficient to reduce the likelihood of a cyber and information security hazard having a relevant impact on the asset (see section 8G of the SOCI Act). This could mean, for example, that an entity needs to take further steps than are set out within the cyber security framework documents to mitigate cyber and information security hazards.

Subsection 11(3) specifies that a responsible entity for a relevant critical infrastructure asset must include a process or system within the CIRMP that complies with a framework specified in the table below subsection 11(3) (including any associated conditions within the time period specified in subsection 7(2)). The frameworks contained in documents specified in the table below subsection 11(3) are to be complied with as they exist in force from time to time. Responsible entities may utilise a framework other than those mentioned in a document in the table below subsection 11(3) in accordance with subsection 11(5), where the alternate framework is equivalent to the framework contained in a document specified in the table.

The purpose of subsection 11(3) is to provide baseline cyber frameworks which responsible entities for relevant critical infrastructure assets must demonstrate compliance with in their CIRMP. Responsible entities may choose one document in the table below subsection 11(3), and must additionally ensure any conditions for that document, specified in the table for that document, are met (paragraph 11(3)(a)).

The 12 month time period provided for in paragraph 11(3)(b) provides a responsible entity with additional time to meet any conditions mentioned in the table for the applicable cyber frameworks in their CIRMP. Paragraph 11(3)(b) provides that the conditions must be met within 12 months after the end of the applicable period mentioned in subsection 7(2).

For example, if the instrument commences on 1 January 2026, then a responsible entity for a relevant critical infrastructure asset on this date will have to comply with Part 2A from 1 July 2026. The responsible entity will then have a further 12 months to comply with the requirements in either subsection 11(3) or subsection 11(5) of the instrument—being 1 July 2027. If an asset becomes a critical infrastructure asset on 1 March 2026 (i.e. became a relevant critical infrastructure asset after the instrument commenced), the responsible entity will be required to comply with this provision after a total of 18 months from that date—1 September 2027.

The note under subsection 11(3) clarifies that sections 30AN and 30ANA of the SOCI Act provide for the incorporation of documents mentioned in this subsection as in force from time to time. The note clarifies that by virtue of sections 30AN or 30ANA of the SOCI Act, this subsection may, despite subsection 14(2) of the Legislation Act, make provision in relation to a matter by applying, adopting or incorporating, with or without modification any matter:

- contained in a standard proposed or approved by Standards Australia as in force or existing from time to time;

Authorised Version Explanatory Statement registered 11/03/2025 to F2025L00325

- contained in a relevant document (see subsection 30ANA(2) of the SOCI Act) as in force or existing from time to time.

Subsection 14(2) of the Legislation Act states that unless the contrary intention appears, the legislative instrument or notifiable instrument may not make provision in relation to a matter by applying, adopting or incorporating any matter contained in an instrument or other writing as in force or existing from time to time. The contrary intention required to incorporate documents by reference, or as they exist from time to time, as per subsection 14(2) of the Legislation Act is contained in sections 30AN and 30ANA of the SOCI Act.

This means that all documents prescribed under subsection 11(3) reflect the most up-to-date versions of those documents for the purpose of complying with CIRMP requirements, even if they are amended after the commencement of this instrument.

Subsection 11(4) specifies that a CIRMP for a critical telecommunication asset that is owned or operated by a carrier must include a process or system that complies with a framework mentioned in the table below section 11(4) (including any associated conditions within the time period specified in subsection 7(2)). The note under subsection 11(4) clarifies that sections 30AN and 30ANA of the SOCI Act provide for the incorporation of documents mentioned in this subsection as in force from time to time.

Subsection 14(2) of the Legislation Act states that unless the contrary intention appears, the legislative instrument or notifiable instrument may not make provision in relation to a matter by applying, adopting or incorporating any matter contained in an instrument or other writing as in force or existing from time to time. The contrary intention required to incorporate documents by reference, or as they exist from time to time, as per subsection 14(2) of the Legislation Act is contained in sections 30AN and 30ANA of the SOCI Act.

The 24 month time period provided for in paragraph 11(4)(b) provides a responsible entity for a critical telecommunications asset owned or operated by a carrier additional time to meet any conditions mentioned in the table for the applicable cyber frameworks in their CIRMP. Paragraph 11(4)(b) provides that the conditions must be met within 24 months after the end of the applicable period mentioned in subsection 7(2).

The obligations in subsection 11(4) for CIRMPs of critical telecommunications assets owned or operated by a carrier assets apply in addition to those obligations specified in subsection 11(3). In effect both subsection 11(3) and subsection 11(4) apply to a CIRMP for critical telecommunications asset owned or operated by a carrier. Responsible entities may utilise a framework other than those mentioned in a document in the table below subsection 11(4) in accordance with subsection 11(5), where the alternate framework meet the conditions expressed in that subsection.

The purpose of this provision is to provide for a higher cyber baseline for a subset of critical telecommunications assets, which is appropriate to address the heightened risk environment faced by these assets.

Authorised Version Explanatory Statement registered 11/03/2025 to F2025L00325

Subsection 11(5) provides that a responsible entity for an asset mentioned in subsection 11(3) or subsection 11(4) may otherwise comply with subsection 11(3) or 11(4) by establishing and maintaining a process or system in the entity's CIRMP that is equivalent to a framework in a document mentioned in the tables, including any conditions.

In effect subsection 11(5) allows for a responsible entity to utilise an alternative framework to those mentioned in the tables below subsection 11(3) and subsection 11(4) to satisfy the requirements of those subsections where the alternate framework, including any conditions, is equivalent to a specified framework.. The onus to prove the equivalency of the alternate framework rests with the responsible entity and must be expressed within the entity's CIRMP. Where an entity applies an equivalent framework, the CIRMP should specify why that document has been chosen and what steps have been taken to ensure that the alternative is equivalent to a document specified in the table.

The purpose of subsection 11(5) is to provide responsible entities with the flexibility to comply with their statutory obligations by recognising alternative cyber security frameworks that achieve the desired uplift in security and resilience of the relevant critical infrastructure asset for the purposes of their Part 2A obligations.

Section 12 Personnel hazards

Section 12 of the instrument specifies, for paragraph 30AH(1)(c) of the SOCI Act, requirements with respect to personnel hazards that must be addressed in the CIRMP for relevant critical infrastructure assets.

Subsection 12(1) provides that a CIRMP for a relevant critical infrastructure asset must include a process or system for personnel hazards that:

- identifies the entity's critical workers (defined in section 5 of the SOCI Act) (paragraph 12(1)(a));
- permits critical workers access to critical components of the relevant critical infrastructure asset only where the critical worker has been assessed as suitable for such access (paragraph 12(1)(b)); and
- as far as reasonably practicable to do so, minimise or eliminate material risks arising from malicious or negligent employees or contractors and arising from the off-boarding process for outgoing employees and contractors (paragraph 12(1)(c)).

Subsection 12(2) provides that in accordance with subsections 30AKA(1), 30AKA(3) and 30AKA(5) of the SOCI Act, a responsible entity must have regard to whether the CIRMP lists the entity's critical workers and whether the CIRMP describes the personnel risks, the occurrence of which could have a relevant impact on the asset.

Authorised Version Explanatory Statement registered 11/03/2025 to F2025L00325

Section 13 Background checks

Subsection 13(1) provides that for the purposes of paragraphs 30AH(1)(b) and 30AH(4)(a) of the SOCI Act, the process or systems for assessing the suitability of a critical worker may be a background check conducted under the AusCheck scheme.

The effect of subsection 13(1) is that responsible entities may utilise a background check conducted under the AusCheck scheme to satisfy the obligation that the entity establish and maintain a process or system in the CIRMP to assess the suitability of a worker as specified in paragraph 12(1)(b).

The note under subsection 13(1) provides that responsible entities are not required to utilise the AusCheck scheme to assess the suitability of critical workers. Responsible entities are entitled to use other measures to assess the suitability of critical workers where the associated process or system for suitability assessment is included and explained in the CIRMP in accordance with paragraph 12(1)(b).

Irrespective of whether an AusCheck background check is utilised as process or system for considering the suitability of critical workers under paragraph 12(1)(b), a responsible entity in making a suitability assessment, must consider the matters set out in subsection 13(4).

Subsection 13(2) provides for the matters which must be included in an AusCheck background check in circumstances where a CIRMP permits an AusCheck background check to be conducted in accordance with subsection 13(1). The information to be assessed must include information relating to:

- those matters mentioned in paragraphs 5(a), 5(b), 5(c) and 5(d) of the AusCheck Act (Paragraph 13(2)(a));
- information relating to the individual's criminal history to be assessed against the criminal history criteria (as defined in section 4 of the instrument) for the purposes of paragraph 30AH(4)(c) of the SOCI Act (paragraph 13(2)(b)); and
- information relating the identity of the individual consisting of both an electronic identity verification check and an in person identity check for the purposes of paragraph 30AH(4)(d) of the SOCI Act (paragraph 13(2)(c)).

Paragraphs 5(a), 5(b), 5(c) and 5(d) of the AusCheck Act concern the definition of 'background check' and what information is sought whilst undertaking a background check as part of the AusCheck scheme.

Subsection 13(3) provides an obligation for responsible entities to notify the Secretary if a relevant background check for the purposes of section 30AH(1)(b) and 30AH(4)(a) of the SOCI Act is no longer required for a critical worker. The purpose of this subsection is to ensure that a responsible entity is actively managing and updating the status of their background checks, including those of outgoing employees and contractors.

Authorised Version Explanatory Statement registered 11/03/2025 to F2025L00325

Subsection 13(4) provides that a responsible entity must consider the matters specified in this subsection when assessing whether a critical worker is suitable to have access to critical components of a relevant critical infrastructure asset in accordance with paragraph 12(1)(b). For this purpose a responsible entity must consider:

- any advice from the Secretary under paragraphs 21DA(2)(a), 21DA(2)(b), subsection 21DA(4) and subsection 21DA(5) of the AusCheck Regulations (paragraph 13(4)(a));
- whether permitting the critical worker access to the critical components of the relevant critical infrastructure asset would be prejudicial to security (paragraph 13(4)(b)); and
- any other information that may affect the person's suitability to access the critical components of the relevant critical infrastructure asset (paragraph 13(4)(c)).

Responsible entities must consider these matters, regardless of whether a background check under the AusCheck scheme was utilised. The phrase 'any advice' in paragraph 13(4)(a) acknowledges that such advice from the Secretary will not be provided in all cases. However, where it is, it must be considered by the responsible entity, as well as the matters mentioned in paragraphs 13(4)(b) and 13(4)(c) when making a suitability assessment.

This subsection requires responsible entities to consider the security risk of an individual. Where the AusCheck scheme is utilised, the background check will provide relevant information to enable them to take steps to control or limit access to the critical infrastructure asset, as required.

The note under subsection 13(4) provides additional context to the reader. The note clarifies that a responsible entity may be required to inform the Secretary of a decision to grant or revoke access to a critical infrastructure asset in certain circumstances. The note directs the reader to section 21ZA of the AusCheck Regulations which outlines the obligation on responsible entities to inform the Secretary of certain decisions under those Regulations.

Subsection 13(6) provides that for the purposes of section 13 the term "Secretary" has the same meaning as in subsection 4(1) of the AusCheck Act.

Section 14 Supply chain hazards

Section 14 of the instrument specifies, for paragraph 30AH(1)(c) of the SOCI Act, requirements with respect to supply chain hazards a CIRMP for a relevant critical infrastructure asset must address.

Paragraph 12(1)(a) of the instrument, provides that the process or system in a CIRMP for a relevant critical infrastructure asset must, as far as it is reasonably practicable to do so, minimise or eliminate the following material risks with respect to supply chain hazards:

- unauthorised access, interference or exploitation of the asset's supply chain (subparagraph (i));
- misuse of privileged access to the asset by any provider in the supply chain (subparagraph (ii));

Authorised Version Explanatory Statement registered 11/03/2025 to F2025L00325

- disruption of the asset due to an issue in the supply chain (subparagraph (iii));
- arising from threats to people, assets, equipment, products, services, distribution and intellectual property within supply chains (subparagraph (iv));
- arising from major suppliers (subparagraph (v)); and
- any failure or lowered capacity of other assets and entities in the entity's supply chain (subparagraph (vi)).

Paragraph 14(1)(b) of the instrument, provides that a CIRMP must, as far as it is reasonably practicable to do so, mitigate the relevant impact of a supply chain hazard on the asset. These requirements are intended to ensure that a CIRMP addresses vulnerabilities in an entity's supply chain in areas such as security, suppliers and logistics. Telecommunications assets usually have particularly complex supply chains, incorporating overseas manufactured specialist hardware and offshore personnel or artificial intelligence in key network management functions.

Subsection 14(2) of the instrument provides that, for subsections 30AKA(1), (3) and (5) of the Act, a responsible entity must have regard to the following matters:

- whether the CIRMP lists the entity's major suppliers (paragraph (a)); and
- whether the supply chain hazards, which could have a relevant impact on the asset, are described in the CIRMP (paragraph (b)).

In accordance with this provision, a responsible entity should consider whether their CIRMP adequately identifies hazards throughout the supply chain that could impact the availability, integrity, reliability or confidentiality of the critical infrastructure asset if they were to occur.

Section 15 Physical security hazards and natural hazards

Section 15 of the instrument specifies, for paragraph 30AH(1)(c) of the SOCI Act, requirements with respect to physical security hazards and natural hazards a CIRMP for a relevant critical infrastructure assets must address.

Subsection 15(1) of the instrument provides that, for physical security hazards and natural hazards, the process or system in a CIRMP for a relevant critical infrastructure asset must:

- identify the physical critical components of the critical infrastructure asset (paragraph (a)); and
- as far as it is reasonably practicable—to minimise or eliminate the material risk of:
    - a physical security hazard on a physical critical component (subparagraph (b)(i)); and
    - a natural hazard on the asset (subparagraph (b)(ii)); and

Authorised Version Explanatory Statement registered 11/03/2025 to F2025L00325

- respond to incidents where unauthorised access to a physical critical component occurs (paragraph (c)); and

- control access to physical critical components, including restricting access to only those individuals who are critical workers or accompanied visitors (paragraph (d)); and

- test that security arrangements for the asset are effective and appropriate to detect, delay, deter, respond to and recover from a breach in the arrangements (paragraph (e)).

The purpose of subsection 15(1) is to require responsible entities to develop processes or systems in their CIRMP for managing and mitigating a variety of physical security hazards and natural hazards to their critical infrastructure assets.

A 'physical critical component', as mentioned in section 15, specifically refers only to those tangible or material parts of an asset where the absence of, damage to or compromise of the part would prevent the proper function of the asset or could cause significant damage to the asset (as defined by section 5 of the SOCI Act). This is in contrast to a critical component (as defined in section 5 of the SOCI Act), which also encompass intangible assets, such as software and computer data, which would not be considered physical critical components for the purpose of section 15 of the instrument.

An example of a physical critical component is a backhaul transport and transmission facilities. These facilities are used to connect remote parts of the network servicing end-users to the core network infrastructure. Any damage to these facilities could prevent the supply of carriage service to the public. A critical component under the SOCI Act would include software used in within the management plane, network virtualisation or edge computing that support the function of backhaul, as well as the physical transmitters and receivers integral to carriage services across Australia. Subsection 15(2) of the instrument provides that, for subsections 30AKA(1), (3) and (5) of the Act, a responsible entity must have regard to whether:

- the asset's physical critical components are described in the CIRMP (paragraph (a));

- the physical hazards, the occurrence of which could have a relevant impact on a physical critical component, are described in the CIRMP (paragraph (b));

- the security arrangements for the asset are described in the CIRMP (paragraph (c)); and

- the natural hazards, the occurrence of which could have a relevant impact on the physical critical components of the asset, are described in the CIRMP (paragraph (d)).

Under this provision, a responsible entity should consider whether their CIRMP adequately identifies and details the physical security hazards and natural hazards that could impact the availability, integrity, reliability or confidentiality of their physical critical components.

Authorised Version Explanatory Statement registered 11/03/2025 to F2025L00325

Part 4 Responsible entity to notify certain changes and proposed changes to telecommunications service or system

Section 16 Application provision

Section 16 is an application provision that enlivens the requirement to notify certain changes and proposed changes to a telecommunication service or system for the purpose of subsection 30EC(1) of the SOCI Act.

Assets that are considered critical telecommunications assets for the purpose of this Part are telecommunications assets that are owned or operated by a carrier. A carrier is defined in the Telecommunications Act as an entity that is the holder of a carrier license granted under section 56 of the Telecommunications Act.

Section 30EC of the Act requires a responsible entity to notify the Secretary as soon as practicable after becoming aware that the implementation of a change, or proposed change, by the entity to a telecommunications service or a telecommunications system is likely to have a material adverse effect on the entity's capacity to comply with its obligation under section 30EB.

The purpose of section 16 is to turn on the notification requirements in section 30EB of the SOCI Act for responsible entities for a critical telecommunications asset that is owned or operated by a carrier.

Section 17 Notification requirements

Section 17 outlines the information that is required to be provided by an entity to the Secretary as required by paragraph 30EC(2)(d) of the SOCI Act.

Subsection 30EC(1) of the SOCI Act requires that a responsible entity for a critical telecommunications asset, prescribed in section 16 of the instrument, to notify the Secretary as soon as practicable after becoming aware of changes to telecommunication services or systems that is likely to have a material advise effect on the entity's capacity to comply with subsection 30EB(2).

Subsection 30EB(2) provides that a responsible entity for critical telecommunications prescribed in rules are required to, so far as it is reasonably practicable to do so, protect the prescribed critical telecommunications asset to ensure the confidentiality of communications (as defined within the Telecommunications Act) carried on, and of information contained on, the prescribed critical telecommunications asset. The entity must also, so far as it is reasonably practicable, protect the asset to ensure the availability and integrity of the prescribed critical telecommunications asset.

Subsection 30EC(2) of the SOCI Act provides that the responsible entity for the prescribed telecommunications asset must, as soon as reasonably practicable after becoming aware of the change or proposed change, notify the secretary in writing of the change or proposed change. The notification must specify the asset and include a description of the change or proposed change and include in the notification any other information of a kind prescribed by the rules for the purposes of this paragraph.

Authorised Version Explanatory Statement registered 11/03/2025 to F2025L00325

Subsection 17(1) of the instrument provides that a responsible entity must provide all information that is reasonably necessary for the Secretary to make an assessment of the change or proposed change. This is a positive obligation on the responsible entity to ensure that the information required to make an assessment regarding the change or proposed change is provided.

Subsection 17(2) outlines the type of information that, as far as it is reasonably practicable to do so, should be provided to the Secretary. However, the list is non-exhaustive and further information can be provided to the Secretary if it is reasonably necessary for the Secretary to make an assessment of the change or proposed change. The types of information specified for this purpose are explained below.

Paragraph 17(2)(a) requires an entity to provide a risk assessment of the changes or proposed changes that consider material risks, supply chain hazards, physical security and natural hazards, personnel hazards, cyber hazards and information hazards. All of these hazards or risks that should be considered for inclusion are reflective of the requirements required in existing CIRMPs.

Paragraph 17(2)(b) requires a responsible entity to provide written evidence demonstrating how the responsible entity evaluated how controls could minimise or eliminate hazards or materials risks identified within the risk assessment for the change or proposed changes. Furthermore, the written evidence must demonstrate that the responsible entity has assessed the material risks of other changes that could achieve the intended project outcome.

Paragraph 17(2)(c) requires a responsible entity to provide details on all software and hardware that is introduced, utilised, changed or affected by the change or proposed change. Information provided regarding software should include, but is not limited to, version numbers for the relevant operating systems and other major software components.

Paragraph 17(2)(d) requires a responsible entity to provide details regarding any major supplier relevant to the project. This includes contracts or outsourcing arrangements that relate to each new hardware element, software element or third part service arrangement.

Paragraph 17(2)(e) requires a responsible entity to provide detailed schematics and system documentation in relation to the change or proposed change. The detailed schematics and system documentation must describe (where relevant):

- interfaces with existing elements of the critical telecommunications asset (subparagraph 17(2)(e)(i);
- security controls (subparagraph 17(2)(e)(ii));
- how business critical data used in connection with any computer introduced by the proposed change is used or stored (subparagraph 17(2)(e)(iii)); and
- network-to-network interfaces with third party systems, including other critical telecommunications assets (subparagraph 17(2)(e)(iv)).

Authorised Version Explanatory Statement registered 11/03/2025 to F2025L00325

Paragraph 17(2)(f) requires a responsible entity to provide details regarding the timeline of planning, development and implementation of the proposed change.

Paragraph 17(2)(g) requires the responsible entity to provide any other information they consider relevant for the Secretary to make an assessment with regard to changes or proposed changes.

The notification obligation is intended to promote a flexible and mutual understanding across industry and government. To give an example of each provision in practice, a carrier is proposing to procure a new contract to outsource certain network management functions offshore. Their notification may include;

- a detailed risk assessment of the change, with emphasis on the material risk that access to operational information offshore may have a relevant impact on the asset if controls aren't sufficient;
- a separate vendor supply chain risk assessment for all vendors involved in the change (including updates to assessments of existing vendors should new locations and/or technologies be introduced in the change);
- how carrier-identified material risks will be mitigated and why the proposed change is preferable to services from other suppliers;
- how access by third-parties to communications networks will be managed and monitored;
- how access logs will be recorded, reviewed and irregularities investigated/actioned;
- details of mechanisms demonstrating how the carrier's Australia-based staff will maintain ultimate control over the network management functions, and if necessary, an explanation detailing how the change is consistent with their obligation to maintain effective control and competent supervision over their networks and facilities;
- what hardware/software is introduced by the change and how remote access will be limited;
- schematics or system documentation of the above;
- when the change is proposed to occur and when key milestones are expected to occur, including once the change is live; and
- anything else the entity considers relevant.

Authorised Version Explanatory Statement registered 11/03/2025 to F2025L00325

Attachment B

Statement of Compatibility with Human Rights

Prepared in accordance with Part 3 of the Human Rights (Parliamentary Scrutiny) Act 2011

Security of Critical Infrastructure (Telecommunications Security and Risk Management Program) Rules (LIN 25/010) 2025

This Disallowable Legislative Instrument is compatible with the human rights and freedoms recognised or declared in the international instruments listed in section 3 of the *Human Rights (Parliamentary Scrutiny) Act 2011.*

Overview of the Disallowable Legislative Instrument

Legislative authority

The *Security of Critical Infrastructure (Telecommunications Security and Risk Management Program) Rules 2025* (TSRMP Rules), are made under section 61 of *Security of Critical Infrastructure Act 2018* (the SOCI Act). This provision allows the Minister to make, by legislative instrument, rules prescribing matters required or permitted by the Act, or that are necessary or convenient to be prescribed for carrying out or giving effect to the Act.

Legislative setting

The *Security of Critical Infrastructure and Other Legislation Amendment (Enhanced Response and Prevention) Act 2024* (the ERP Act) amended the SOCI Act to uplift, align and enhance key security obligations from Part 14 of the *Telecommunications Act 1997* (Telecommunications Act) into the SOCI Act. This enables the government to maintain its ability to oversee, and intervene into (where appropriate), the telecommunications industry to ensure national security outcomes and to clarify security obligations under a single regulatory framework.

The ERP Act introduced three key enhanced security obligations for critical telecommunications assets to integrate existing obligations from the Telecommunications Act into the SOCI Act. These were:

1. a ‘protect your asset’ obligation, which requires the protection of assets for security purposes and from all hazards, identified by the entity, as far as it is reasonably practicable to do so;
2. a notification obligation which requires responsible entities to notify the Secretary of Home Affairs of security risks incurred by network changes or planned changes to the critical telecommunications asset or network; and
3. a requirement that specified assets are to comply with obligations under Part 2A of the SOCI Act. This provided for the introduction, through subordinate legislation, of a bespoke Telecommunications Security Risk Management Program (TSRMP).

The TSRMP Rules implement the above enhanced security obligations for critical telecommunications assets, and will be enlivened upon the commencement of Schedule 5 of the ERP Act, which contains the enabling provisions upon which the TSRMP Rules rely.

TSRMP Rules purpose and background

The SOCI Act requires owners and operators of critical infrastructure assets to meet positive security obligations and comply with government directions in response to security incidents, when certain thresholds and requirements are met. The TSRMP Rules, by operationalising elements of Part 2A and Part 2D of the

Authorised Version Explanatory Statement registered 11/03/2025 to F2025L00325

SOCI Act, provide a framework of security obligations specifically tailored to a sub-set of critical telecommunications assets – i.e. those that are owned, or operated by, a carrier or a relevant carriage service provider (*relevant critical infrastructure assets*) – to help mitigate against the unique hazards that may affect the communications sector. When operationalised in relation to *relevant critical infrastructure assets*, Part 2A of the SOCI Act will require responsible entities to adopt, maintain and comply with a risk management plan and Part 2D of the SOCI Act will impose specific security protection and notification obligations on the responsible entities, as outlined in the TSRMP Rules.

Emerging risks are rapidly outpacing the current regulatory environment in the telecommunications sector. The purpose of the TSRMP Rules is to enhance government and industry understanding of the threat environment facing Australia's critical telecommunications assets, and build the security and resilience of these assets against security incidents that would adversely impact businesses and the Australian economy. The TSRMP Rules seek to minimise the security and economic impact on industry from its ongoing exposure to risk. The Department has prepared an impact analysis for the TSRMP Rules as an addendum to the 2022 *Regulation impact statement: a risk management framework for critical infrastructure assets*.

The cost to Australia's critical telecommunications assets extends beyond the responsible entities themselves in the event of a serious incident. One event could have a catastrophic impact on the ability for a critical telecommunications assets to service Australia, which would in turn have cascading impacts across society and the entire Australian economy.

In order to raise the security for *relevant critical infrastructure assets*, the TSRMP Rules require responsible entities for *relevant critical infrastructure assets* to:

- specify critical telecommunications asset which, for the purposes of the obligation to protect said asset as outlined in section 30EB of the SOCI Act, a responsible entity must comply with;
- identify all material risks to their asset across four key hazards domains (cyber and information, personnel, supply chain, and physical security and natural hazards) and minimise or eliminate those risks so far as it is reasonably practical to do so;
- meet certain governance requirements;
- 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 through compliance with specified frameworks;
- identify critical workers and assess their suitability to access critical components of the asset;
- address vulnerabilities in the supply chain;
- establish and maintain in their risk management program a process or system to address physical security and natural hazards; and
- include certain information as part of the obligation to notify the Secretary of changes or proposed changes to the telecommunications service or system.

The TSRMP Rules also provide for a compliance grace period, which suspends application of Part 2A of the SOCI Act for *relevant critical infrastructure assets* until the later of six months after the commencement of the TSRMP Rules, or six months after the asset becomes a relevant critical infrastructure asset.

Consultation

Subsections 30ABA(2) and 30AL(2) of the SOCI Act require the Minister for Home Affairs (the Minister) to publish a notice on the Department of Home Affairs' website setting out the draft TSRMP and inviting persons to make submissions to the Minister about the draft TSRMP or amendments during a consultation period no shorter than 28 days. The Minister opened consultation on the draft TSRMP for 60 days from 16

Authorised Version Explanatory Statement registered 11/03/2025 to F2025L00325

December 2024 to 14 February 2025 inclusive. The Minister gave a copy of the notice to the First Minister of each State and Territory.

Minor changes were made as a result of the consultation process. These changes clarified the operation of section 11, which relates to cyber and information hazards.

The Minister considered all submissions received within the consultation period and was satisfied that appropriate consultation was undertaken, in accordance with section 17 of the *Legislation Act 2003.*

Human rights implications

This Disallowable Legislative Instrument engages the right to privacy in Article 17 of the *International Covenant on Civil and Political Rights* (ICCPR).

Article 17(1) of the ICCPR provides that no one shall be subjected to arbitrary or unlawful interference with their privacy.

Requiring responsible entities to give information and notify of changes

Rule 5 of the TSRMP Rules defines, for the purposes of the Rules, a *relevant critical infrastructure asset* as a critical telecommunications asset. This definition imposes (when the ERP Act amendments are operationalised by making an instrument for Schedule 5) additional requirements on critical telecommunications assets to provide personal information, as detailed below.

Rules 9(2)(c), 9(2)(d) and 11(1)(a) of the TSRMP Rules require responsible entities of *relevant critical infrastructure assets* to identify the contact details of its critical positions and critical personnel in their TSRMP. Critical personnel, for example, may be a senior executive or technical expert within the responsible entity. This requires responsible entities to collect and store personal information, including the names of certain employees.

Rule 15 of the TSRMP Rules clarifies the information relevant to an entity's circumstances that must be provided to the Secretary under the obligation to notify of certain changes and proposed changes to a telecommunications service or system. This includes a risk assessment of the change or proposed change which considers, including but not limited to, personnel hazards. While collection of personal information is not specifically called out in the list of change notification triggers, it is possible that collection, storage and disclosure of personal information will be required as part of the notification obligation. For example, in notifying of a change, such as outsourcing network management functions, a responsible entity could include personal information as part of their risk assessment.

Requiring responsible entities to give information, including the contact details for critical positions and critical personnel, and notify of changes which consider, including but not limited to, personnel hazards, helps ensure relevant risks to *relevant critical infrastructure assets* can be mitigated. For example this will allow the most critical personnel to be quickly identified immediately prior, during, or following, a significant telecommunications incident in order to manage risk. Critical personnel have responsibility, access, control and/or management of the essential components or systems of *relevant critical infrastructure asset*s and may fulfil an important role in restoring proper functioning subsequent to a significant telecommunications incident, where the absence or compromise of critical personnel may have a cascading impact on proper functioning of the asset.

Requiring responsible entities to give information, including the contact details for critical positions and critical personnel, and notify of changes to personnel hazards, is also necessary to protect public order and

Authorised Version Explanatory Statement registered 11/03/2025 to F2025L00325

national security, as it assists to protect *relevant critical infrastructure assets* from 'trusted insiders' who may disrupt the provision of telecommunications services. Trusted insiders are potential, current or former employees, or contractors, who have legitimate access to information, techniques, technology, assets or premises. Trusted insiders can intentionally or unknowingly assist external parties in conducting activities against the *relevant critical infrastructure asset* or can commit malicious acts of self-interest. Such action by a trusted insider can undermine or severely impact the availability, integrity, reliability or confidentiality of those assets captured as *relevant critical infrastructure assets*. Requiring responsible entities to give information, including the contact details for critical positions and critical personnel, and notify of changes to personnel hazards, enables the Secretary to ensure that the responsible entity has the proper processes in place to support the quick revocation or amendment of access to critical systems and physical components if a potential malicious insider is identified. Personal details may be shared with law enforcement agencies in response to an incident to assist consequence management and incident response.

Appropriate safeguards exist to ensure any use of personal information is reasonable, necessary and proportionate. Under these measures the responsible entity is only required, where specified, to collect, store and disclose contact details for personnel deemed critical, which safeguards against the arbitrary collection, storage and disclosure of personal information.

Information and documents provided to the Secretary is protected information and the use and disclosure is restricted in line with provisions at Part 4, Division 3 of the SOCI Act. Where protected information is personal information, disclosure will only be permitted where it is for a specified purpose and authorised by a specific provision under the SOCI Act, in accordance with a direction issued under the SOCI Act or otherwise authorised by law. Part 4, Division 3, Subdivision B of the SOCI Act provides criminal penalties to deter the disclosure of protected information.

Further, safeguards for the protection of personal informational specified in the Australian Privacy Principles (APPs) in Schedule 1 of the *Privacy Act 1988* apply to interest and control information, as well as operational information gathered under Part 2 and Part 4 of the SOCI Act. This includes requirements regarding the security of personal information specified under Australian Privacy Principle 11 and requirements regarding use or disclosure under Australian Privacy Principle 6.

To the extent that the TSRPM Rules, under these measures, enable a responsible entity of a *relevant critical infrastructure asset* to collect, store and disclose of personal information for the purpose giving information and notifying of changes, the right to privacy will be engaged. Any limitation on the right to privacy however is permissible because the collection, storage and disclosure of personal information will be lawful, will not be arbitrary, and will be reasonable, necessary and proportionate to the legitimate objective of protecting national security and public order. Further, the measures are proportionate and the least rights restrictive because the use and disclosure provisions of the SOCI Act will continue to operate in harmony with the Privacy Act to limit disclosure to circumstances where it is necessary and for an authorised purpose.

Background checks

The TSRMP Rules require responsible entities to establish and maintain a process to assess the suitability of critical workers to have access to critical components of a *relevant critical infrastructure asset*. When the ERP Act amendments are operationalised pursuant to Schedule 5, rule 11(2) of the TSRMP Rules will enable a responsible entity to conduct an AusCheck background check on critical workers for that purpose. The

Authorised Version Explanatory Statement registered 11/03/2025 to F2025L00325

AusCheck background check may also enable the responsible entity to ensure only persons suitable to such a role are engaged as critical employees.

The collection, use and disclosure of personal information for the purpose of an AusCheck background check is authorised by the *AusCheck Act 2007* and the *AusCheck Regulations 2017*. When an AusCheck background check is conducted, personal information is provided voluntarily by an individual with their express consent to it being used for the purpose of the background check, and the individual is provided a privacy notice by AusCheck detailing how their information will be used, thereby ensuring the individual's consent is fully informed.

The use of the AusCheck scheme is optional, and the responsible entity for the asset may use other schemes or processes for background checking. Responsible entities are not obligated to use background checking services in managing personnel risks, if sufficient alternative processes are in place. It is up to individual entities to decide how best to assess the personnel risks workers pose, and how to manage these risks.

If entities choose to use a non-AusCheck background check, or use another process for background checking, the entity is responsible for ensuring that the third-party provider complies with contractually determined privacy protections in relation to the collection, use and disclosure of personal information. This may include such measures as inclusion of a policy or process in the contract with the third party for dealing with personal data. In such situations, a critical worker would need to consent to their personal information being shared with a third party service provider. If operating in Australia, that third-party provider would also have requirements under the *Privacy Act 1998* to comply with the Australian Privacy Principles.

To the extent that the TSRMP Rules enable a responsible entity of a *relevant critical infrastructure asset* to disclose an individual's personal information to AusCheck for the purpose of a background check, the right to privacy will be engaged. Additionally, if a responsible entity decides to use another scheme or process for background checking, the right to privacy will be engaged. Any limitation on the right to privacy however is reasonable, necessary and proportionate to legitimate objective of mitigating against the material risk and impact personnel hazards could have on *relevant critical infrastructure assets* and the essential services delivered by them, such as a compromise to the confidentiality, reliability, availability or integrity of that asset. Further, the measures are proportionate and the least rights restrictive because it is limited to workers who are engaged as critical workers, where the responsible entity considers it necessary for the position, and because the availability of AusCheck background checks, or other background checks or processes as the responsible entity decides is appropriate, is dictated by threat risk.

Conclusion

The Disallowable Legislative Instrument is compatible with human rights because to the extent that it may limit human rights, those limitations are not arbitrary or unlawful and are reasonable, necessary and proportionate to pursue the legitimate objective of national security and public order.

The Honourable Tony Burke MP
Minister for Home Affairs
Minister for Cyber Security

Authorised Version Explanatory Statement registered 11/03/2025 to F2025L00325

Attachment C

Supplementary analysis for Critical Telecommunications Assets

Overview of the role of telecommunications in Australia

Telecommunications assets are central to social and economic activity in Australia.[1] Industry, government and individuals make daily use of services enabled by telecommunications networks and related assets, which involve the electronic transmission of data and information between users. Telecommunications assets are relied on and share interdependencies with all critical infrastructure sectors and are particularly important to:

- banking and finance;
- healthcare;
- logistics;
- energy transmission; and
- government and defence activities, including disaster responses.

The COVID-19 pandemic and an increasing occurrence of significant natural disasters have reaffirmed the importance of reliable telecommunications assets. Disruptions, including by sabotage, causes significant impacts on reliant critical services and end-users. Further, telecommunications assets store and transmit highly sensitive Australian data, making them a primary target for espionage activities.

Impacts of a disruption to telecommunications assets

Disruptions to telecommunications assets can cause a wide array of consequences, including:

- In the case of **natural disasters,** which typically damage above-ground network components and energy supply, public safety risks may arise if:
  - the public are unable to receive emergency warnings via national warning systems;
  - telecommunications networks are overloaded, making it difficult for essential calls to be connected; or
  - there are delays in restoring telecommunications assets, where telecommunications carriers have to wait for safe conditions to repair systems or provide temporary telecommunications facilities.
- The realisation of other **physical risks** may result in the reduced or suspended operation of a telecommunications asset. Outages may be nation-wide and include:
  - outages to payment systems;
  - no access to emergency services;
  - downstream asset outages if they rely on data storage or cloud services to function; and
  - disrupted supply chains, including in freight and food and grocery sectors.
- Where a **cyber-attack** occurs, telecommunications assets holding sensitive data may be compromised. Where an asset also maintains cloud and data services for corporate customers, a cyber-attack may allow access to these corporations' systems and consequently, compromise of their commercial or customer data. A cyber-attack may also allow hostile adversaries access to sensitive law-enforcement and intelligence related data, including interception capability plans prepared in compliance with the *Telecommunications (Interception and Access) Act 1979.*
- With **complex supply chains** and increasing integration between international networks, software and hardware, telecommunications assets are experiencing increasing challenges in identifying, managing and responding to supply chain risks and vulnerabilities. Insolvency, international trade disruptions or other risks affecting critical suppliers can impact an asset's ability to continue operations efficiently. Further, complex supply chains can generate security risks such as entry points through compromised hardware products.

[1] Australian Infrastructure Audit 2019 - 8. Telecommunications.pdf, pg556.

Authorised Version Explanatory Statement registered 11/03/2025 to F2025L00325

These consequences are considered in further detail in the following case studies from both Australian and international contexts.

Examples of disruptions to telecommunications assets – domestic and international

2022 Optus data breach	Cyber Risk

Situation: In September, 2022, Optus suffered a cyber-attack which led to the theft of customer data. The breach occurred due to an unsecured application interface that allowed other devices and systems to access it.[2] The stolen customer data contained personal information data such as addresses, Medicare information, passport information and driver licences.

Outcome: The incident impacted approximately 10 million current and former Optus customers to varying degrees, with some having to replace several identification documents following the breach. In November 2022, Optus announced it had made a provision for exceptional expenses of $140 million for action to prevent harm to customers.[3]

A class action seeking damages for impacted customers was launched in 2023 with over 100,000 participants, claiming that Optus breached consumer and telecommunications law and failed its duty of care to protect its customers' information. The class action may cause additional direct impacts to Optus.[4]

Identified Gap: The impact of the Optus data breach on its customers highlighted a greater need for adequate risk management processes and stronger systems to improve the resilience of networks to data breaches and improve the reliability of networks.

2022 Cyber-attack on Satellite Network in Ukraine[5]	Cyber Risk

Situation: On February 24, 2022, a cyber-attack disrupted broadband satellite internet access throughout Ukraine. This attack disabled modems that communicate with ViaSat Inc's KA-SAT, a critical Ukrainian satellite network, which supplies internet access to tens of thousands of people in Ukraine and Europe. The attack was deliberately designed to disrupt Ukrainian command and control services. The remote malware deployed in the system created impacts throughout Europe, by remotely erasing software on modems and routers making them non-operational.

Outcome: The attack impacted telecommunications systems, threatened government and military objects, and impacted civilian objects both in Ukraine and beyond when they experienced a loss of internet access and disruptions to energy systems. While most network users were back online after several days, some users reported that their internet access was unavailable for more than two weeks.[6]

Critical infrastructure throughout Europe was impacted, including a German energy company who lost remote monitoring access to over 5,800 wind turbines. In France, nearly 9,000 subscribers of a satellite internet service provider experienced outages. An additional 13,000 subscribers of other satellite internet service providers across Hungary, Greece, Italy, and Poland were affected.

Identified Gap: This case study demonstrates the need for regulation to consider all hazards, including from malicious actors that could disrupt a network. Telecommunications assets should be required to anticipate and respond to disruption by malicious actors, including undertaking risk management activities which may prevent or mitigate flow on impacts.

[2] Optus data breach, Queensland Government, 2022.

[3] Optus Half Year results, Optus, 2022.

[4] Slater and Gordon commences class action against Optus over data breach, Slater and Gordon media release, 2023,

[5] Case Study: Viasat Attack, cyberconflicts, 2022.

[6] KA-SAT Network cyber attack overview, 2022.

Authorised Version Explanatory Statement registered 11/03/2025 to F2025L00325

2019-2020 Bushfires Impact on Major Australian Telecommunication Networks	Natural Hazard
Situation: In 2019–20, unprecedented fires swept across Australia's south-east coast. The fires impacted many communities and critical services, including telecommunications. These disruptions created significant challenges for individuals and communities seeking emergency assistance and access to Government-issued emergency alerts, as well as general welfare communications.[7]	
Outcome: The magnitude of the fires saw significant damage to physical telecommunications assets. It was reported that 1,390 facilities were impacted, with the average outage lasting 3.5 days.[8] Prolonged power outages created major disruption, including for those seeking to aid recovery. Loss of network coverage meant that people were unable to receive emergency messages about the location of fires. This affected people's ability to make decisions about preparing their properties, whether to evacuate, and where to evacuate to. Emergency services had reduced communications and had to rely on radiocommunications in many instances.[9]	
Identified Gap: Consistent regulatory standards across all critical infrastructure assets may mitigate the impact of mass outages, including through enhancing knowledge and understanding of the incident response mechanisms available where a risk to a telecommunications asset is realised.	

[7] Final-Report-of-the-NSW-Bushfire-Inquiry.pdf, NSW Government.

[8] Impacts of the 2019-20 bushfires on the telecommunications network, ACMA, 2020; Final-Report-of-the-NSW-Bushfire-Inquiry, NSW Government.

[9] Impacts of the 2019-20 bushfires on the telecommunications network, ACMA, 2020; Final-Report-of-the-NSW-Bushfire-Inquiry, NSW Government.

Authorised Version Explanatory Statement registered 11/03/2025 to F2025L00325

2022 Outage of Critical Japanese Mobile Carrier	Supply Chain Risk
Situation: On July 2, 2022, KDDI Corp, Japan's second-largest mobile carrier, experienced a network disruption. The disruption lasted for more than 60 hours and impacted more than 40 million mobile customers' (including 260,000 corporate users) ability to make phone calls and access internet services.[10]	
Outcome: Investigations found the disruption occurred as a result of a malfunction in equipment used for voice call services. Beyond the direct impacts felt by KDDI Corp's customer base, the outage created significant flow on impacts to other essential services. This included, for example, disruption to weather service providers reliant on KDDI's network, temporary cessation of postage services and parcel deliveries, inability to access ATMs and use network-connected vehicles.[11] Payment systems were also affected by the outage.[12]	
Identified Gap: This case study highlights the importance of regulatory frameworks which enhance industry-wide resilience through consistent risk management activities. Where reliance on a single provider can be reduced, and adequate risk management mechanisms are in place, the impacts of disruptions can be mitigated.	

Outline of four key hazard domains

Hazard Domain	Identified Risk	Hypothetical Example
Physical & Natural	Increased occurrence of extreme weather events and natural disasters including heatwaves, bushfires and floods means that telecommunications assets are exposed to natural hazard risks. These risks have the potential to damage both physical infrastructure and remote systems.	Floods can cause significant disruptions to telecommunications assets including, reduced ability to deliver and support critical services following disaster events until connectivity is restored.
Supply chain	Disruptions to telecommunications assets' supply chains can affect Australia's social and economic stability, defence, and national security, as well as the reliability and security of other critical infrastructure assets. This risk is magnified where organisations are primarily reliant on supplies that are sourced internationally.	A telecommunications provider may be reliant on a sole or limited number of third-party suppliers for critical hardware components used in the operations of its assets. Where this major supplier faces disruptions, the quality, security, and ability to provide telecommunication services may be compromised. This may lead to widespread service disruptions for many customers if the supplier's component was unable to be delivered or malfunctions (and no alternative is available).
Personnel	Personnel with advanced knowledge, access to systems, data or premises may pose insider threat risks including espionage, infrastructure sabotage and misuse of sensitive data.	An employee may access sensitive information or compromise network availability. This could result in theft or exposure of sensitive information. The telecommunications provider may face consequences such as service disruptions,

[10] KDDI aims to restore service, Reuters, 2022.

[11] Telecom network outages, the ESG risks of a connected world, 2022, Sustainalytics.

[12] KDDI aims to restore service, Reuters, 2022.

Authorised Version Explanatory Statement registered 11/03/2025 to F2025L00325

Hazard Domain	Identified Risk	Hypothetical Example
		data breaches, reputational damage and legal liability.
Cyber	Telecommunication assets are vulnerable to thousands of attempted cyber-attacks every day. Due to constant improvements in infiltration capabilities, it has become easier to carry out destructive cyber-attacks.	A telecommunications provider faces a cyber-attack by a group of malicious actors who aim to disrupt communication networks and steal sensitive data. The attack exploits vulnerabilities within the company's software, network and employee devices to gain unauthorised access to company data.

Existing legislation related to Telecommunications assets and entities of the Australian Telecommunications Sector

Overview of Regulation		Identified Gaps
Security of Critical Infrastructure Act 2018	The SOCI Act manages national security risks in Australia's critical infrastructure assets. The SOCI Act applies to eleven sectors including communications, data storage and processing and energy. The SOCI Act establishes: • the requirement to adopt and maintain a written risk management program; • reporting requirements in the event of cyber incidents which impact on the availability, integrity, reliability, and confidentiality of the asset to the Australian Cyber Security Centre; • obligations to provide operational and ownership information to the Register of Critical Infrastructure Assets; • last resort government assistance measures for incident response. • measures to protect sensitive information about critical assets; • enhanced Cyber Security Obligations' applied to 'Systems of National Significance' (SoNS).	Critical telecommunications assets are not currently subject to obligations under the SOCI Act, except any enhanced cyber security obligations that are applied to declared SoNS. Where they are not SoNS, critical telecommunications assets are currently only subject to the obligation to notify data storage providers if they store or process business critical data.

Authorised Version Explanatory Statement registered 11/03/2025 to F2025L00325

Overview of Regulation		Identified Gaps
Telecommunications Act 1997	The Telecommunications Act 1997 (Tel Act) establishes a regulatory framework for carriers and carriage service providers. Carriage services are defined as services for carrying communications by means of guided and/or unguided electromagnetic energy. The Act imposes obligations for: • protecting the privacy of communications; • preventing telecommunications networks to be used to commit offences; and • facilitating the use of carriage services for defence purposes or the management of natural disasters. Additionally, Part 14 sections 313(1A), 314A & 314B, and sections s315A, 315B and 315C require telecommunication providers to do their best to protect the security of their networks and facilities, including to stop their use in criminal acts. Under Part 14, the ACMA can investigate and take enforcement action if providers fail to comply with obligations and improperly use information and documents that come into their possession in the course of their business which relate to the contents of a communication: • that has been or is being carried; • was supplied by the carriage service; or • details a person's personal affairs. Sections 313(1A), 314A and 314B, and section 315A under the Tel Act will be integrated into the SOCI Act through these reforms.	The Tel Act imposes a diverse range of responsibilities on carriers and carriage service providers, particularly in relation to privacy and in states of emergency. However, the Act does not include any specific requirement to develop and implement risk management programs. While interim reporting obligations have been switched on under Tel Act, there are generally no reporting obligations on captured entities. The Act instead mandates that providers submit information to the Register of Critical Assets or comply with Mandatory Cyber Incident reporting.

Authorised Version Explanatory Statement registered 11/03/2025 to F2025L00325

Overview of Regulation		Identified Gaps
Privacy Act 1988	The Privacy Act 1988 (Privacy Act) dictates how personal information in the federal public sector and in the private sector can be collected, used, stored, and disclosed.	The Privacy Act is the primary lever for the protection of personal information, given its unique ability to regulate the large-scale collection and distribution of data. While it provides avenues for individuals to complain about alleged interferences with their privacy by service providers, it does not impose positive obligations on telecommunications providers to create and implement risk management protocols.
Radiocommunications Act 1992	The Radiocommunications Act 1992 regulates the planning, allocation, and use of radiocommunications. The Act provides for: • radio frequency planning; • licencing and registration of radiocommunications; • re-allocation of parts of the spectrum; and • general regulatory requirements extending to equipment rules, interference with radiocommunications and dispute management.	Complaints can be made to the Australian Communications and Media Authority (ACMA) where there is an interference or risk of interference or disruption to radiocommunications. While ACMA has a range of powers to respond to risks, there is no requirement to create a risk management program or reporting requirement. Similarly, licence holders have a compliance reporting obligation to the ACCC, but this does not extend to risk management protocols.
Telecommunications (Interception and Access) Act 1979	The Telecommunications (Interception and Access) Act 1979 (TIA Act) makes it an offence to intercept or access private telecommunications without the knowledge of those involved in that communication, except for law enforcement or national security purposes.	While the TIA Act does impose risk minimisation duties on the Director-General of Security in relation to the issuance of foreign communications warrants, as well as on ACMA in granting exemptions for trial services, there is no specific requirement for risk management protocols for telecommunications sector disruptions.
Foreign Acquisitions and Takeovers Act 1975	The Foreign Acquisitions and Takeovers Act 1975 mandates that foreign individuals must obtain approval to operate or own telecommunications services in Australia.	The Act provides last resort powers to deal with foreign investment-borne national security risks and to penalise officers where there were high risks of contravention of the Act. However, the FATA is not designed to directly consider the risk management activities of Australia's critical infrastructure and cannot address the identified gaps.

Authorised Version Explanatory Statement registered 11/03/2025 to F2025L00325

Existing standards, guidelines, and regulators for Australia's telecommunications sector

Organisation	Standards & guidelines
Department of Infrastructure, Transport, Regional Development, Communication and the Arts	Telecommunications (Carrier Licence Conditions – Security Information) Declaration 2022 Telecommunications (Carriage Service Provider – Security Information) Determination 2022
The Communications Access Co-ordinator (within the Attorney-General's Department, under TIA Act)	Interception capability plan to be lodged annually by 1 July

Jurisdiction	Regulators
Commonwealth	Department of Home Affairs Department of Infrastructure, Transport, Regional Development, Communication and the Arts Australian Communications and Media Authority (ACMA) Australian Competition and Consumer Commission (ACCC) Telecommunications Industry Ombudsman Australian Information Commissioner Attorney-General's Department Communications Alliance

Costing process completed by responsible entities for critical telecommunications assets

Industry participants were consulted on the proposed regulatory changes and rules from Q1 2024. Feedback from the initial consultation was incorporated into this Supplementary Analysis.

To assess the potential cost implications of the proposed regulatory changes, an additional consultation period was held between 15 December 2024 and 14 February 2025. This consultation period sought submissions from Industry participants on the cost impacts of the proposed regulatory changes. This additional consultation resulted in limited engagement and no submissions on the estimated cost impact. Noting the nil response, the Department has adopted a qualitative analysis of the potential impacts to industry and the broader economy of the proposed regulatory option.

This qualitative assessment will draw on the previous analysis from the 2022 Regulatory Impact Assessment (RIS) of the then proposed regulatory changes to the SOCI Act. It is estimated that the cost to implement the regulatory changes for critical telecommunications assets would not be more than, and is likely to be less than, that of the regulatory changes for other critical infrastructure assets (and which were examined in the 2022 SOCI RIS).

Likely net benefit – option 2

The following section details the costs and benefits associated with option 2 (the regulatory option) before assessing the overall likely net benefit presented by this option.

Authorised Version Explanatory Statement registered 11/03/2025 to F2025L00325

Costs of option 2

The cost of regulation will be borne by responsible entities for critical telecommunications assets who meet the threshold in the Rules. The direct costs of regulation have been assessed against the cost impact rating scale in the table below. For each element of the proposed regulatory change, an assessment of the scale of cost impact to industry has been made.

Community organisations and individuals will not be directly affected but there will likely be indirect costs passed onto consumers. Without quantification of the direct cost impact, an assessment of the indirect impact is difficult. For the purposes of this Supplementary Analysis, consideration of the indirect impact has been limited to commentary on the economic analysis undertaken for the other critical infrastructure asset classes examined in the 2022 SOCI RIS.

Cost impact rating scale

Cost Impact Rating	Description
Low	The required uplift or change to an entity's processes, capability, governance and systems is minor. The requirements of SOCI are being substantively met by current activities and consequently, the marginal cost of implementing and maintaining compliance with the SOCI obligations is Low.
Moderate	The required uplift or change to an entity's processes, capability, governance and systems is significant in some but not all areas of the business. The requirements of SOCI are being partially met by current activities and consequently, the marginal cost of implementing and maintaining compliance with the SOCI obligations is Moderate.
High	The required uplift or change to an entity's processes, capability, governance and systems is significant in most areas of the business. The requirements of SOCI are not being met by current activities and consequently, the marginal cost of implementing and maintaining compliance with the SOCI obligations is High.

Assessment of cost impact to critical infrastructure assets

Proposed changes	Cost Impact Rating	Rationale
Introduce an all hazards critical infrastructure risk management program	Moderate	The introduction of the critical infrastructure risk management program would require industry to uplift current practices to ensure compliance with the SOCI Act. Existing telecommunications security requirements already require risk mitigation, particularly against sabotage and espionage and cyber security. The CIRMP is an all-hazards obligation, so some uplift is still required. It is therefore assessed that this broader obligation would have a moderate impact to industry.
Addition of new reporting requirements to ensure compliance with the amended regulations.	Low	This change would require industry participants to produce a board or equivalent attested report annually on their written CIRMP. Noting the frequency of this and that most (or all) affected entities will already have significant risk management activities in place, this change has been assessed as having a low impact.

Authorised Version Explanatory Statement registered 11/03/2025 to F2025L00325

Based on the above assessment, it is estimated that the cost to implement the regulatory changes for critical telecommunications assets would not be more than, and is likely to be less than, that of the regulatory changes implemented for other critical infrastructure assets (and which were examined in the 2022 SOCI RIS). Given the existing regulatory framework established by the Tel Act, owners of critical telecommunications assets are already subject to security obligations involving risk management and reporting requirements. While the SOCI Act integrates and uplifts these obligations to an all-hazards framework, it is assessed that the cost impact will be lower than for other classes of critical infrastructure asset because the processes, capabilities, governance and systems required to comply with the new obligations will only require uplift rather than establishment. For most entities this will result in a lower cost impact relative to the estimated costs presented in the 2022 SOCI RIS.

In this context, a summary of the cost impact data collected during the 2021-22 consultation period[13] is provided below.

Regulatory cost per entity from 2021-22 consultation period (indexed to December 2024)

Critical infrastructure asset	Costs ($ million)	
	Average one-off cost per entity (submissions)	Average annual ongoing cost per entity (submissions)
Critical electricity assets	9.3	4.4
Critical gas assets	12.1	2.4
Critical water assets	16.5	7.0
Critical data processing or storage assets	2.0	2.2
Critical broadcasting and domain name system assets	0.8	0.6
Critical financial market infrastructure assets (payment systems)	0.1	1.6
Critical liquid fuels assets	10.2	3.0
Critical hospitals	14.9	11.6
Critical energy market operator assets	25.4	7.7
Critical freight infrastructure *and* critical freight services assets	4.5	2.6
Critical food and grocery assets	3.6	2.0
Total average cost per entity	**9.0**	**4.1**

Benefits of option 2

Reliable and continuous access to telecommunications assets is critical for Australia's prosperity. The critical infrastructure risk management program framework will uplift baseline security across all captured critical telecommunications assets to ensure more resilience to hazards. Its primary benefit is that compliance with the risk management program reduces the frequency and intensity of incidents, which has cascading whole of economy benefits by minimising supply disruptions and economic shocks.

Economic impacts of disruptions to telecommunications assets

Disruptions to critical telecommunication assets can have profound effects, both directly on customers and as other critical infrastructure assets are unable to use telecommunications networks to perform essential

[13] Information about the methodology for calculating the costs from 2021-22 consultation period can be found in the 2022 RIS.

Authorised Version Explanatory Statement registered 11/03/2025 to F2025L00325

services. These events generate costly immediate and longer-term impacts on the Australian economy. Further, telecommunications assets hold significant quantities of data including highly sensitive data about all Australians and entities. As such, telecommunications assets may be more frequently exposed to risks involving attempted espionage and sabotage than other critical infrastructure assets.

A significant incident affecting a critical telecommunications asset may cause:

- disruptions to economic activity, with immediate impacts on other critical infrastructure or government services (e.g. financial intermediaries, health, and transport services);
- self-perpetuating economic shocks through the supply chain if redundancies are unavailable or inadequate;
- compromises to sensitive data, including business critical data, which may generate further national security and privacy risks and severe opportunity costs as business efforts are redirected to consequence management; and
- impairments of the availability of networks causing wide-ranging communications difficulties for individuals, including but not limited to:
    - connecting with friends and family,
    - contacting health care and emergency services,
    - obtaining information or advice,
    - working from home, or
    - undertaking online educational courses.

Additionally, a disruption to telecommunications infrastructure can significantly affect the social well-being of Australia. The case studies above show that disruptions to telecommunications assets can have an amplified negative impact on communities during existing emergency situations such as floods and bushfires. Consequently, in addition to the costs to the economy of a disruption to telecommunication assets, there are the community costs of death, disease or, injury which are increased in consequence or likelihood because of an incident.

With Government and businesses increasingly storing and communicating large amounts of information on and across critical telecommunications assets, these assets have increasingly become a target for espionage, sabotage, and interference activity. In instances where this information is unlawfully accessed, sensitive data, law enforcement operations, and the location of persons could be exposed.

To support the assessment of the potential direct and indirect economic impacts of an incident to a critical telecommunications asset on the Australian economy, a series of case studies were included in this Supplementary Analysis. These case studies highlight that telecommunications outages inflict substantial direct and indirect costs on firms and households alike. Businesses bore the brunt of the damage across all case studies, mostly through lost income and productivity. It is clear from the case studies noted above that industrial and commercial sectors can be significantly impacted by telecommunication outages.

For the purposes of estimating the cost of a range of future avoided incidents in Australia, an incident impacting a ‘Major Telecommunications Carrier’ was used. Given the magnitude of damages, this incident is considered a moderate risk scenario. The use of an incident modelled on an actual event to define a baseline risk point of comparison is important because it ensures the benefits analysis is grounded in reality.

Based on this, a framework for considering the potential impacts of Australian telecommunication asset outages following failure of critical infrastructure is provided in the table below.

	Severe scenario	Moderate scenario	Low scenario
Intensity of event	200% of moderate scenario	Incident impacting Major Telecommunications Carrier	50% of moderate scenario

As noted above, the economic impact of an incident will vary due to a range of factors including the location and type of incident, as well as its timing and duration. While an incident with a much greater impact than the severe scenario is conceivable, the defined scenarios and subsequent benefits analysis are based on a deliberately conservative approach to ensure the severe scenario remains demonstrably plausible. Due to this, this analysis may not incorporate all direct costs incurred by all future incidents.

Authorised Version Explanatory Statement registered 11/03/2025 to F2025L00325

	Scenario 1 (Severe) $ million	Scenario 2 (Moderate) $ million	Scenario 3 (Low) $ million
Total direct cost to the economy of the incident	$280	$140	$70
Total in-direct costs to the economy of the incident	50-75% of the direct cost.		

In the broader context of a potential future disruption, in addition to the above estimate of benefits would be the avoided costs of recovery (repair costs, costs of resulting mitigations, productivity loss due to attending to legal ramifications, intangible costs on the environment, health and wellbeing, loss of reputation etc.).It is estimated that there would be additional indirect costs of an incident due to both the upstream and downstream of the supply chain impacts. Based on the economic modelling undertaken for other classes of critical infrastructure assets in the 2022 RIS, the additional indirect costs could range from 50-75% of the total direct costs of an incident.

Further, the increasing frequency of incidents makes the proposed risk management program framework more certain over time to exceed the anticipated costs. The examples referred to above demonstrate the increasing need for adequate protections against the security and resilience of critical telecommunications assets, and the increased likelihood that the benefits of the draft risk management program framework will exceed the costs outlined in this section.

Assessment of likely net benefit

The likely benefits of option 2 will be at least (and are expected to be more than) the costs of the regulation. This is primarily because, the frequency and severity of all hazard risks for telecommunication assets are growing. While some events of the magnitude described in this Supplementary Analysis have previously been considered to represent the worst-case disruption scenarios in Australia, the increasing severity and frequency of similar incidents, particularly in the context of growing cybersecurity incidents, represents a risk to the whole economy.

The cost for critical telecommunications assets is likely to be less than for the other classes of critical infrastructure asset examined in the 2022 SOCI RIS because the Tel Act already requires some of the processes, capabilities, governance and systems which will be required by rules and obligations established by the SOCI Act. This, together with the increasing frequency of incidents, makes the proposed risk management program framework more likely to exceed the anticipated costs over time.

Further, through pursuit of option 2, the identification, mitigation and remediation of such hazards, should they occur, will be improved through:

- lowering the material risk of hazards and subsequent impacts of those hazards, as they manifest for critical telecommunication assets; and
- ensuring that adoption of the risk management program framework for telecommunication assets is reasonable and proportionate to the purpose of the program;

Overall, these factors and the specific costs and benefits described above mean the likely net benefit associated with option 2 is high.

Authorised Version Explanatory Statement registered 11/03/2025 to F2025L00325