EXPLANATORY STATEMENT

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

Security of Critical Infrastructure Act 2018

Security of Critical Infrastructure Amendment (2025 Measures No. 1) Rules 2025

Legislative authority

The *Security of Critical Infrastructure Amendment (2025 Measures No. 1) Rules 2025* are made under section 61 of the *Security of Critical Infrastructure Act 2018* (the SOCI Act).

The instrument amends the following legislative instruments:

- *Security of Critical Infrastructure (Application) Rules(LIN 22/026) 2022* (Application Rules); and
- *Security of Critical Infrastructure (Critical infrastructure risk management program) Rules (LIN 23/006) 2023* (CIRMP Rules).

The amendments are made in accordance with subsection 33(3) of the *Acts Interpretation Act 1901.* That subsection provides that a power to make a legislative instrument includes a power to amend of repeal that instrument in the same manner, and subject to the same conditions, as the power to make the instrument.

The instrument commences as follows, in accordance with the table set out in section 2:

- Sections 1 to 4 and anything else in the instrument not elsewhere covered in the table commence on the day after registration;
- Schedule 1 and Schedule 2 to the instrument commence on the later of the day after the instrument is registered, and immediately after the commencement of Parts 1 and 2 of Schedule 5 to the *Security of Critical Infrastructure and Other Legislation Amendment (Enhanced Response and Prevention) Act 2024* (ERP Act).

The instrument is a legislative instrument for the purposes of the *Legislation Act 2003*.

Purpose

Positive security obligations—Parts 2, 2A and 2B of the SOCI Act

Part 2 of the SOCI Act provides that the Secretary of the Department must keep a private Register of Critical Infrastructure Assets containing information in relation to those assets. Under Part 2, the responsible entity for a critical infrastructure asset must give operational information, and a direct interest holder in relation to the asset must give interest and control information, to the Secretary to be included in the Register. For paragraph 18A(1)(a) of the SOCI Act, the Application Rules specify the assets to which Part 2 of the SOCI Act applies.

Part 2A of the SOCI Act provides that the responsible entity for one or more critical infrastructure assets, to which Part 2A applies, must have and comply with a critical infrastructure risk management program (**CIRMP)** unless an exemption applies. For paragraph 30AB(1)(a) of the SOCI Act, the CIRMP Rules specify the assets to which Part 2A applies and requirements that responsible entities must comply with.

Authorised Version Explanatory Statement registered 13/03/2025 to F2025L00324

A CIRMP is a written program, the purpose of which, under paragraph 30AH(1)(b) of the SOCI Act, is to require a responsible entity for a critical infrastructure asset:

- to identify each hazard where there is a material risk that the occurrence of the hazard could have a relevant impact on the asset; and
- so far as it is reasonably practicable to do so—to minimise or eliminate any material risk of such a hazard occurring; and
- so far as it is reasonably practicable to do so—to mitigate the relevant impact of such a hazard on the asset.

Part 2B of the SOCI Act provides that if a cyber security incident has a relevant impact on a critical infrastructure asset, the responsible entity for the asset may be required to give a relevant Commonwealth body a report about the incident. For paragraph 30BB(1)(a) of the SOCI Act, the Application Rules specify the assets to which Part 2B applies.

Strengthening protection of data storage systems

This instrument amends the CIRMP Rules to support amendments of the SOCI Act by the ERP Act and to give effect to the legislative reforms outlined under Shield 4 of the 2023-2030 Australian Cyber Security Strategy (ACSS).

The instrument introduces a requirement for the CIRMP of a responsible entity for a critical infrastructure asset to consider the material risk of an impact to the availability, integrity, reliability or confidentiality of data storage systems holding business critical data. It also inserts a note clarifying the application of subsection 9(7) of the SOCI Act (inserted by Schedule 1 to the ERP Act), identifying that certain data storage systems will be taken to be part of a critical infrastructure asset specified in the rules.

The requirement is already applied through the SOCI Act. This amendment provides further clarity that responsible entities are required to include risks to relevant data storage systems within their CIRMP. These amendments clarify required action to support Action 13 of the ACSS; ensuring that critical infrastructure assets are protecting critical data held, used, and processed in ‘business-critical’ data storage systems.

Critical telecommunications assets

The instrument further supports the ERP Act and gives effect to the legislative reforms outlined under Shield 4 of the ACSS through the alignment of the telecommunications sector with other specified critical infrastructure assets in the Application Rules.

Reflecting the migration of telecommunications security regulation from the *Telecommunications Act 1997* to the SOCI Act, this instrument amends the Application Rules to specify that Parts 2 and 2B of the SOCI Act apply to critical telecommunication assets which are owned or operated by a carrier, or owned and operated by a relevant carriage service provider. A relevant carriage service provider asset is a critical infrastructure asset that is owned and operated by a carriage service provider used in connection with the supply of at least 20,000 active total carriage services, or used in the connection

Authorised Version Explanatory Statement registered 13/03/2025 to F2025L00324

with carriage services supplied to a Commonwealth entity (other than a body corporate established by a law of the Commonwealth).

This reflects Action 13 of the ACSS by aligning the positive security obligations of telecommunication providers to the same standards as other critical infrastructure entities.

Part 2A obligations for critical telecommunications assets are separately provided for by the *Security of Critical Infrastructure (Telecommunications Security and Risk Management Program) Rules 2025* (TSRMP Rules).

Compliance with Part 2A obligations through other instruments

The instrument updates the CIRMP Rules to insert a provision which facilitates, in specific circumstances, responsible entities being able to meet their Part 2A obligations other than by meeting the requirements set out in the CIRMP Rules for a critical infrastructure asset specified in the CIRMP Rules.

The requirements for a CIRMP are set out in Part 2 of the CIRMP Rules. These requirements will not apply to an asset specified in that instrument, if its applicable CIRMP complies with the requirements set out in another instrument (for example, the TSRMP Rules) and the responsible entity for the asset is also the responsible entity for an asset specified in the other instrument.

For example, a responsible entity for a critical broadcasting asset specified in the CIRMP Rules may also be the responsible entity for a relevant critical infrastructure asset specified in the TSRMP Rules. The CIRMP requirements set out in Part 2 of the CIRMP Rules will not apply to the critical broadcasting asset, if that critical broadcasting asset has a CIRMP that complies with the requirements set out in Part 3 of the TSRMP Rules. The requirements in the CIRMP must apply to the critical broadcasting asset as if the critical broadcasting asset were a relevant critical infrastructure asset specified in the TSRMP Rules.

This provision acknowledges that it may be preferable for the responsible entities for multiple assets to follow one set of requirements in respect of all of their assets' CIRMPs, while still ensuring that all assets specified for the purposes of Part 2A of the SOCI Act have an appropriate CIRMP.

Details of the instrument

Details of this instrument are set out in Attachment A.

Parliamentary scrutiny etc.

The instrument is subject to disallowance under section 42 of the *Legislation Act 2003*. A Statement of Compatibility with Human Rights has been completed in accordance with the *Human Rights (Parliamentary Scrutiny) Act 2011*. The overall assessment is that the instrument is compatible with human rights. The Statement is included at Attachment B.

Authorised Version Explanatory Statement registered 13/03/2025 to F2025L00324

Consultation

Part 2, 2A and 2B

Sections 18AA, 30ABA and 30BBA of the SOCI Act require that, before making or amending rules under sections 18A, 30AB and 30BB respectively, the Minister must:

- cause a notice to be published on the Department's website that sets out the draft rules or amendments, and invites persons to make submissions to the Minister;
- give a copy of the notice to each State and Territory First Minister; and
- consider any submissions received within the period specified in the notice.

Subsections 18AA(3), 30ABA(3) and 30BBA(3) of the SOCI Act specify that the period of the notice must be no shorter than 28 days.

For rules or amendments under section 30BB, the Minister must also:

- give a copy of the draft rules or amendments to the responsible entity for an asset that is, or is proposed to be, specified in the rules; and
- if a submission is received from these entities within the specified notice period—give the entity a written statement that sets out the Minister's response to the submission.

The Department of Home Affairs (the Department) engaged industry stakeholders responsible for critical telecommunications assets during the development of this amendment.

Before making this instrument, the Minister in accordance with sections 18AA, section 30ABA and section 30BBA of the SOCI Act:

- published a notice on the Department's website that:
    - set out the draft amendment made for the purposes of section 30ABA of the SOCI Act;
    - 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
- provided a copy of the notice to the First Minister of each State and Territory.

Once the consultation period had closed, the Minister considered all submissions received, which included 10 written submissions, nine on the Data Storage Systems amendment and four on the Critical Telecommunications Assets amendment, noting that submissions generally covered more than one amendment. All submissions were reviewed and considered in the making of the amendments.

Impact Analysis

The Office of Impact Analysis was consulted in developing these amendments and considered that they are unlikely to have more than a minor regulatory impact.

Authorised Version Explanatory Statement registered 13/03/2025 to F2025L00324

Attachment A

Details of the *Security of Critical Infrastructure Amendment (2025 Measures No. 1) Rules 2025*

Section 1 Name

Section 1 provides that the title of this legislative instrument is the *Security of Critical Infrastructure Amendment (2025 Measures No. 1) Rules 2025*.

Section 2 Commencement

Section 2 provides for the commencement of the instrument.

Subsection 2(1) provides that each provision of the instrument specified in column 1 of the table commences, or is taken to have commenced, in accordance with column 2 of the table. Any other statement in column 2 has effect according to its terms.

The effect of table item 1 is that sections 1 to 4 and anything else in this instrument not elsewhere covered in the table at section 2, commences on the day after registration of the instrument.

The effect of table items 2 and 3 is that commencement of Schedule 1 and Schedule 2 is contingent on the commencement of Parts 1 and 2 of Schedule 5 to the ERP Act. If the relevant Parts of the ERP Act have commenced, then Schedule 1 and Schedule 2 will commence on the day after this instrument is registered on the Federal Register of Legislation. However, if the relevant Parts of the ERP Act have not yet commenced, the provisions will not commence on the day after this instrument is registered and will instead commence immediately after the commencement of Parts 1 and 2 of Schedule 5 to the ERP Act.

Subsection 2(2) provides that information in column 3 of the table (date/details) is not part of the instrument and may be edited, or information inserted into the column, in any published version of the instrument.

Section 3 Authority

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

Section 61 of the SOCI Act provides that the Minister may, by legislative instrument, make rules prescribing matters that are required or permitted by the Act to be prescribed by the rules, or necessary or convenient to be prescribed for carrying out or giving effect to 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 61 of the SOCI Act therefore authorises the Minister to amend the rules as provided for in this legislative instrument.

Section 4 Schedules

Section 4 provides that each instrument that is specified in a Schedule to this instrument is amended or repealed as set out in the applicable items in the Schedule concerned, and any other item in a Schedule to this instrument has effect according to its terms.

Authorised Version Explanatory Statement registered 13/03/2025 to F2025L00324

Schedule 1 to the instrument amends the *Security of Critical Infrastructure (Critical infrastructure risk management program) Rules (LIN 23/006) 2023* (CIRMP Rules).

Schedule 2 to the instrument amends the *Security of Critical Infrastructure (Application) Rules (LIN 22/026) 2022* (Application Rules).

Authorised Version Explanatory Statement registered 13/03/2025 to F2025L00324

Schedule 1—Amendments of the *Security of Critical Infrastructure (Critical infrastructure risk management program) Rules (LIN 23/006) 2023* (the CIRMP Rules)

Data storage systems and compliance with Part 2A obligations

Item [1] Section 3 (note)

This item repeals the note at the beginning of section 3 and substitutes a new note.

The effect of the new note is to insert the expression 'business critical data' into the list of expressions, used the CIRMP Rules, and which are defined in the SOCI Act.

The expression 'business critical data' is used in new paragraph 6(f) of the CIRMP Rules (inserted by Item 5 of this Schedule) It has the meaning given by section 5 of the SOCI Act.

Item [2] Section 3 (definition of Act)

This item inserts a definition of the expression "Act" in section 3 of the CIRMP Rules.

This clarifies that where the expression "Act" appears in the CIRMP Rules, it is a reference to the SOCI Act.

Item [3] At the end of subsection 4(1)

This item inserts a note at the end of subsection 4(1) which provides that a 'a data storage system that satisfies all of the requirements under subsection 9(7) of the SOCI Act in respect of a critical infrastructure asset specified in subsection (1) is taken to be part of the critical infrastructure asset.'

Subsection (1) in the note refers to subsection 4(1) of the CIRMP Rules; an application provision specifying, pursuant to paragraph 30AB(1)(a) of the SOCI Act, to which critical infrastructure assets Part 2A of the SOCI Act (Critical infrastructure risk management programs) applies.

Subsection 9(7) of the SOCI Act was inserted by the ERP Act, and provides that a data storage system is taken to be part of a critical infrastructure asset 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; and presents a material risk of a relevant impact on the critical infrastructure asset where there is a material risk that the occurrence of 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 in acquitting its CIRMP obligations under Part 2A, in relation to a critical infrastructure asset, a responsible entity 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.

For example, in developing the CIRMP for a critical infrastructure asset it owns or operates, the responsible entity will need to ensure that it includes any data storage system that may be connected to or used in conjunction with that asset and which stores relevant business data. As part of considering risk management and mitigation for the asset, the responsible entity will need to consider mitigations against threats that may have an adverse impact on that system or the data it holds.

The growing number of cyber incidents impacting non-operational data storage systems held by critical infrastructure entities over the past two years has demonstrated the risk to these systems, which hold large quantities of both personal information and other business critical data. While this requirement is already conferred through the SOCI Act, this amendment provides further clarity on

Authorised Version Explanatory Statement registered 13/03/2025 to F2025L00324

the requirement for responsible entities to consider risk holistically within their risk management program, including that posed to and by relevant data storage systems.

Item [4] After subsection 4(3)

This item inserts new subsection 4(4) (Compliance with Part 2A obligations through other instruments) into the CIRMP Rules. This new subsection provides circumstances in which a responsible entity for an asset specified in subsection 4(1) may be compliant with their obligations under Part 2A of the SOCI Act other than by meeting the requirements set out in Part 2 of the CIRMP Rules.

Part 2 of the CIRMP Rules specify, for the purpose of paragraph 30AH(1)(c), the requirements for a critical infrastructure risk management program; including the material risks, general hazards, cyber and information security hazards, personnel hazards, supply chain hazards, and physical security and natural hazards that must be addressed in a risk management program for a critical infrastructure asset.

New subsection 4(4) provides that Part 2 of the CIRMP Rules will not apply to a critical infrastructure asset specified in subsection 4(1) of the CIRMP Rules if:

- an entity is the responsible entity for a critical infrastructure asset specified in subsection 4(1) of the CIRMP Rules (referred to as a 'CIRMP Rule asset'); and
- that entity is also the responsible entity for a critical infrastructure asset specified in another equivalent instrument for the purposes of paragraph 30AB(1)(a) of the SOCI Act; and
- the entity is in compliance with an equivalent instrument for the purposes of paragraph 30AB(1)(a) of the SOCI Act and a risk management program obligation that applies to the CIRMP Rule asset complies with the requirements specified for paragraph 30AH(1)(c) in the other instrument relating to the other asset (as if those requirements related to the asset specified in the CIRMP Rules); and
- the responsible entity complies with the requirements specified for subsections 30AKA(1), (3) and (5) in the other instrument (as if those requirements related to the asset specified in the CIRMP Rules).

For example: an entity is the responsible entity for a critical broadcasting asset specified in the CIRMP Rules and for a relevant critical telecommunications asset specified in the TSRMP Rules. The requirements for a CIRMP set out in Part 2 of the CIRMP Rules will not apply to the critical broadcasting asset, if the critical broadcasting asset has a CIRMP that complies with the requirements set out in Part 3 of the TSRMP Rules. The responsible entity can apply the requirements in the CIRMP specified in the TSRMP Rules to the critical broadcasting asset as if it were a relevant critical asset, and this will be taken to acquit their obligations under Part 2A.

This provision acknowledges that it may be preferable for the responsible entities for multiple assets to follow one set of requirements in respect of all of their assets' CIRMPs. Where this provision is utilised, assets specified for the purposes of Part 2A in the SOCI Act must still be in compliance with the CIRMP obligation for all assets owned or operated by the responsible entity.

Authorised Version Explanatory Statement registered 13/03/2025 to F2025L00324

Item [5] At the end of section 6

This item inserts subsection 6(f), which specifies 'impact to the availability, integrity, reliability or confidentiality of the data storage system holding business critical data' as a material risk for the purpose of subsection 30AH(8) of the SOCI Act.

In accordance with paragraph 30AH(1)(b) of the SOCI Act, this requires responsible entities to:

- identify, in their CIRMP hazards where there is an impact to the availability integrity, reliability or confidentiality of the data storage system holding business critical data;
- establish and maintain a process or system, in their CIRMP, to—so far as it is reasonably practicable to do so—minimise or eliminate the risk of such hazards occurring; and
- establish and maintain a process or system, in their CIRMP, to—so far as it is reasonably practicable to do so—mitigate the relevant impact of such a hazard on the asset.

The item clarifies that, for hazards where there is an impact to the availability, integrity, reliability or confidentiality of a data storage system holding business critical data, the likelihood of occurrence is so high, or the relevant impact on the critical infrastructure asset is so significant, that the risk must be appropriately addressed through a CIRMP. The failure of a responsible entity's CIRMP to minimise or eliminate such hazards may lead to a relevant impact on a critical infrastructure asset (as defined in section 8G of the SOCI Act).

This amendment further implements the intent of Schedule 1 to the ERP Act, which seeks to ensure that critical data held, used, and processed in 'business-critical' data storage systems are recognised and protected as part of critical infrastructure assets.

Authorised Version Explanatory Statement registered 13/03/2025 to F2025L00324

Schedule 2—Amendments of the *Security of Critical Infrastructure (Application) Rules (LIN 22/026) 2022* (the Application Rules)

Item [1] Section 3

This item inserts two new definitions in the appropriate positions in the list of definitions in section 3 of the instrument – ***Act*** *and* ***relevant carriage service provider asset****.*

The definition of the expression ***Act*** clarifies that where the expression "Act" appears in the Application Rules, it is a reference to the *Security of Critical Infrastructure Act 2018.*

The definition of ***relevant carriage service provider asset*** is inserted to support the amendments made by items 2 and 3 of this Schedule.

A "relevant carriage service provider asset" is a critical infrastructure asset which is owned or operated by a carriage service provider, and meets one of the requirements in paragraphs (a) or (b).

Paragraph (a) requires the asset is used in connection with the supply of at least 20,000 active total carriage services. Carriage services include broadband services, fixed telephone services, public mobile telecommunications services and voice only services.

Paragraph (b) requires the responsible entity for the asset is aware that the asset is used in connection with carriage services supplied to a Commonwealth entity. A body corporate established by a law of the Commonwealth is not a Commonwealth entity for the purpose of paragraph (b).

Item [2] Subsection 4(1) (note)

This item repeals the note at the end of subsection 4(1). This is a consequential amendment, supporting the amendment in item [3], which adds a new paragraph 4(1)(n) at the end of subsection 4(1). The note repealed by item [2] now appears as "Note 1" under new paragraph 4(1)(n).

Item [3] At the end of subsection 4(1)

This item adds new paragraph 4(1)(n), which adds a critical telecommunications asset that is:

- owned or operated by a carrier (as defined in the *Telecommunications Act 1997*, per section 5 of the SOCI Act); or
- a relevant carriage service provider asset (as defined in section 3, as amended by item [1] of this Schedule);

to the list of assets specified for the purpose of paragraph 18A(1)(a) of the SOCI Act.

Paragraph 18A(1)(a) of the SOCI Act is an application provision which provides that Part 2 of the SOCI Act (Register of Critical Infrastructure Assets) applies to assets that are specified in the rules.

The effect of paragraph 4(1)(n), therefore, is that Part 2 of the SOCI Act applies to critical telecommunications assets that are owned or operated by a carrier, or are relevant carriage service provider assets.

These assets must be added to the Register of Critical Infrastructure Assets maintained by the Secretary of the Department administering the SOCI Act. Responsible entities for these assets will incur obligations to provide certain information to the Secretary, and to notify the Secretary of certain events, in relation to the assets.

Authorised Version Explanatory Statement registered 13/03/2025 to F2025L00324

Subsection 4(3) of the Application Rules provides a 'grace period' for compliance with Part 2 of the SOCI Act, during which time Part 2 of the SOCI Act does not apply to the critical infrastructure assets. This period begins when the asset becomes a critical infrastructure asset and ends at the later of:

- six months after the commencement of Application Rules (paragraph 4(3)(a)); and
- six months after the asset becomes a critical infrastructure asset (paragraph 4(3)(b)).

As the Application Rules commenced on 8 April 2022, the period under paragraph 4(3)(b) is applicable – that is, six months after the asset becomes a critical infrastructure asset.

Existing critical telecommunications assets that are owned or operated by a carrier, or are relevant carriage service provider assets already have an existing equivalent obligation to report to the Register and must be in compliance.

For relevant critical telecommunications assets which may come into existence in the future, and to which section 18A of the SOCI Act applies, the grace period will end six months after those assets become critical infrastructure assets.

Item [3] also inserts two notes at the foot of subsection 4(1). Note 1 replicates the note that previously appeared under paragraph 4(1)(m) before new paragraph 4(1)(n) was inserted.

New Note 2 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 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; and presents a material risk of a relevant impact on the critical infrastructure asset where there is a material risk that the occurrence of a hazard could have an impact on the data storage system.

Item [4] At the end of subsection 5(1)

This item inserts new paragraph 5(1)(u), which adds a critical telecommunications asset that is:

- owned or operated by a carrier (as defined in the *Telecommunications Act 1997*, per section 5 of the SOCI Act); or
- a relevant carriage service provider asset (as defined in section 3, as amended by item [1] of this Schedule);

to the list of assets specified for the purpose of paragraph 30BB(1)(a) of the SOCI Act.

Paragraph 30BB(1)(a) of the SOCI Act is an application provision that provides that Part 2B of the SOCI Act (Notification of cyber security incidents) applies to assets that are specified in the rules.

The effect of new paragraph 5(1)(u), therefore, is that Part 2B of the SOCI Act applies to critical telecommunications assets that are owned or operated by a carrier, or are relevant carriage service provider assets.

Responsible entities for these assets must report certain cyber security incidents to the relevant Commonwealth body. These include incidents that had, or are having, a significant impact (whether direct or indirect) on the availability of the asset; and incidents that had, are having, or are likely to have, a relevant impact (defined in section 8G of the SOCI Act) on the asset.

Authorised Version Explanatory Statement registered 13/03/2025 to F2025L00324

Existing critical telecommunications assets that are owned or operated by a carrier, or are relevant carriage service provider assets hold an existing equivalent obligation to report cyber security incidents through the *Telecommunications (Carriage Service Provider—Security Information) Determination 2022* and the *Telecommunications (Carrier Licence Conditions—Security Information) Declaration 2022.* These existing instruments under the *Telecommunications Act 1997* will continue to be in effect until 7 July 2025. During the time period in which these two instruments are in effect the obligation to report cyber security incidents remains applicable. After this period, the obligations under Part 2B of the SOCI Act will need to be complied with.

For relevant critical telecommunications assets which may come into existence in the future, and to which section 30BB applies, the grace period will end three months after those assets become critical infrastructure assets.

Authorised Version Explanatory Statement registered 13/03/2025 to F2025L00324

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 Amendment (2025 Measures No. 1) Rules 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 instrument, the *Security of Critical Infrastructure Amendment (2025 Measures No. 1) Rules 2025* (Amendment Rules) is made under section 61 of the *Security of Critical Infrastructure Act 2018* (the SOCI Act).

The instrument amends the following instruments:

- *Security of Critical Infrastructure (Application) Rules (LIN 22/026) 2022* (Application Rules);
- *Security of Critical Infrastructure (Critical infrastructure risk management program) Rules (LIN 23/006) 2023* (CIRMP Rules);

Schedule 1 and Schedule 2 to the instrument commence on the later of the day after the instrument is registered and immediately after the commencement of Parts 1 and 2 of Schedule 5 to the *Security of Critical Infrastructure and Other Legislation Amendment (Enhanced Response and Prevention) Act 2024* (ERP Act). Sections 1 to 4 of the instrument commence on the day after the instrument is registered on the Federal Register of Legislation.

The instrument is a legislative instrument for the purposes of the *Legislation Act 2003.*

Legislative framework

Positive security obligations—Parts 2, 2A and 2B of the SOCI Act

Part 2 of the SOCI Act provides that the Secretary of the Department must keep a private Register of Critical Infrastructure Assets (Register) containing information in relation to those assets. Under Part 2, the responsible entity for a critical infrastructure asset must give operational information, and a direct interest holder in relation to the asset must give interest and control information, to the Secretary to be included in the Register. For paragraph 18A(1)(a) of the SOCI Act, the Application Rules specifies the assets to which Part 2 of the SOCI Act applies.

Part 2A of the SOCI Act provides that the responsible entity for one or more critical infrastructure assets, to which Part 2A applies, must have and comply with a critical infrastructure risk management program (CIRMP) unless an exemption applies. For paragraph 30AB(1)(a) of the SOCI Act, the

Authorised Version Explanatory Statement registered 13/03/2025 to F2025L00324

CIRMP Rules specifies the assets to which Part 2A applies and requirements that responsible entities must comply with.

A CIRMP is a written program, the purpose of which, under paragraph 30AH(1)(b) of the SOCI Act, is to require a responsible entity for a critical infrastructure asset:

- to identify each hazard where there is a material risk that the occurrence of the hazard could have a relevant impact on the asset; and
- so far as it is reasonably practicable to do so—to minimise or eliminate any material risk of such a hazard occurring; and
- so far as it is reasonably practicable to do so—to mitigate the relevant impact of such a hazard on the asset.

Part 2B of the SOCI Act provides that if a cyber security incident has a relevant impact on a critical infrastructure asset, the responsible entity for the asset may be required to give a relevant Commonwealth body a report about the incident. For paragraph 30BB(1)(a) of the SOCI Act, the Application Rules specifies the assets to which Part 2B applies.

The ERP Act

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* (ACSS). The ERP Act amendments sought to strengthen security and reliability of the critical infrastructure sector in response to recent cyber-security attacks which exposed gaps in the regulatory framework.

The ERP Act amended the SOCI Act to:

- expand the definition of all types of critical infrastructure assets to include secondary assets which hold 'business critical data' and relate to the functioning of the primary asset; and

- bring appropriate elements of the Telecommunications Sector Security Reforms (TSSR) administered by the Home Affairs portfolio, including security and notification obligations, from Part 14 of the *Telecommunications Act 1997* into the SOCI Act, with enhancements to align the regulatory frameworks and clarify telecommunications-specific obligations.

Amendment Rules' purpose and background

The Amendment Rules make various amendments to both the CIRMP Rules and Application Rules to operationalise amendments made by the ERP Act relating to data storage systems and critical telecommunications assets. The specific amendments made by the Amendment Rules are outlined below.

Data storage systems

The Amendment Rules amend the CIRMP Rules to strengthen security obligations across critical infrastructure assets by specifying that impacts to the availability, integrity, reliability or confidentiality of data storage systems holding business critical data, are material risks for the purpose of CIRMPs. As specified above, responsible entities who hold obligations to hold and maintain a CIRMP must identify each hazard where there is a material risk of that hazard occurring.

By providing that hazards to data storage systems, where there is a material risk of the kind specified in the Amendment Rules, must be considered in an entity's CIRMP, the Amendment Rules ensure adequate protection of data storage systems related to critical infrastructure assets, and reflect Action

Authorised Version Explanatory Statement registered 13/03/2025 to F2025L00324

13 of the ACSS; ensuring that critical infrastructure assets are protecting critical data held, used, and processed in 'business-critical' data storage systems.

Critical telecommunications assets

The Amendment Rules further support the amendments made by the ERP Act, and give effect to the legislative reforms outlined under Shield 4 and Action 13 of the ACSS, by aligning positive security obligations for responsible entities of critical telecommunications assets with those of other critical infrastructure assets in the Application Rules.

The Amendment Rules clarify the definition of a 'critical telecommunications asset' and 'relevant carriage service provider asset' for the purposes of the SOCI Act, and enliven positive security obligations (see below) for critical telecommunications assets owned or operated by a carrier and for a subset of critical telecommunication assets owned or operated by a carriage service provider (CSP). The purpose of applying positive security obligations to a subset of assets owned or operated by a CSP (as opposed to all CSPs) is to ensure providers who deliver limited services are not subject to undue regulatory burden. Overall, these amendments made by the Amendment Rules reflect the significant importance of certain telecommunications assets to Australia's critical infrastructure.

SOCI Act, Part 2 (Register of Critical Infrastructure Assets)

The Amendment Rules amend subsection 4(1) of the Application Rules to enliven requirements in Part 2 of the SOCI Act for critical telecommunications assets (carriers and relevant CSP assets). As specified above, where a critical infrastructure asset is prescribed in the Application Rules for the purpose of section 18A, the Secretary must keep a register containing information relating to those assets. Enlivening Part 2 requirements for critical telecommunications assets (carriers and relevant CSP assets) also imposes positive obligations on responsible entities for those assets to give information to the Secretary for this purpose, and to notify the Secretary if particular events occur.

SOCI Act, Part 2B (notification of cyber security incidents)

The Amendment Rules also amend subsection 5(1) of the Application Rules to enliven the requirements in Part 2B of the SOCI Act for critical telecommunications assets (carriers and relevant CSP assets). As outlined above, where a critical infrastructure asset is specified in the Application Rules for this purpose, responsible entities of those assets are subject to mandatory reporting requirements where a cyber security incident occurs which has had, or is having, a significant impact on the availability of the 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 Rules or amendments and inviting persons to make submissions to the Minister about the draft Rules or amendments during a consultation period no shorter than 28 days. The Minister opened consultation on the draft amendments for 60 days from 16 December 2024 to 14 February 2025 inclusive. The Minister gave a copy of the notice to First Minister of each State and Territory. The Minister considered all submissions received within the consultation period.

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).

Authorised Version Explanatory Statement registered 13/03/2025 to F2025L00324

Article 17 of the ICCPR provides that no one shall be subjected to arbitrary or unlawful interference with their privacy. Interferences with privacy may be permissible provided that it is authorised by law and is not arbitrary. For an interference with the right to privacy not to be arbitrary, the interference must be for a reason consistent with the provisions, aims and objectives of the ICCPR and be reasonable in the particular circumstances. The United Nations Human Rights Committee has interpreted 'reasonableness' in this context to mean that 'any interference with privacy must be proportional to the end sought and be necessary in the circumstances of any given case'. The term unlawful means that no interference can take place except as authorised under domestic law.

The Amendment Rules may engage the right to privacy for:

- responsible entities (owners or operators) for an asset
- the responsible entity's employees, or
- the responsible entity's customers/consumers.

Data storage systems

Subsection 9(7) of the SOCI Act provides that a data storage system is taken to be part of a critical infrastructure asset 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; and
- presents a material risk of a relevant impact on the critical infrastructure asset where there is a material risk that the occurrence of a hazard could have an impact on the data storage system.

By clarifying that obligations under Part 2A of the SOCI Act, in relation to a critical infrastructure asset, also need to take into account data storage systems, if the data storage system satisfies the requirements under subsection 9(7) of the SOCI Act, the Amendment Rules, by amending the CIRMP Rules*,* require responsible entities to consider data storage systems as part their CIRMP. This is further supported by the Amendment Rules in so far as it further amends CIRMP Rules to expand, for the purpose of CIRMPs, under Part 2A of the SOCI Act, the definition of 'material risk' as including 'impact to the availability, integrity, reliability or confidentiality of the data storage system holding business critical data'.

The growing number of cyber incidents impacting non-operational data storage systems held by critical infrastructure entities recently has demonstrated the risk to these systems, which hold large quantities of both personal information and other business critical data. To the extent that information about personnel or customers may be recorded in a data storage system taken to be part of a critical infrastructure asset, the Amendment Rules may engage the right to privacy. The Amendment Rules, by clarifying that data storage systems captured by subsection 9(7) of the SOCI Act must be considered as part of a CRIMP, and by clarifying 'material risk' in relation to data storage systems for the purpose of a CRIMP, promote the right to privacy for individuals who have their personal information recorded by enhancing positive security obligations for responsible entities as they relate to data storage systems.

Critical Telecommunications Assets

For critical infrastructure assets specified in the Amendment Rules, responsible entities are required to report ownership and operational information to the Register (Part 2, Division 2 of the SOCI Act), and

Authorised Version Explanatory Statement registered 13/03/2025 to F2025L00324

report cyber incidents to the Australian Signal Directorate's Australian Cyber Security Centre (ACSC) (Part 2B of the SOCI Act). By amending Application Rules to 'switch on' these obligations for responsible entities of critical telecommunications assets (carriers and relevant CSP assets) the Amendment Regulations may engage the right to privacy.

Register - obligation to give information and notify of events

The 'switching on' of Register obligations for responsible entities of critical telecommunication assets (carriers and relevant CSP assets), means responsible entities must provide ownership and operational information to the Secretary of Home Affairs, and notify the Secretary of certain events, in relation to the assets. This may involve incidental disclosure of personal information in relation to who ultimately controls or influences an asset though ownership, including beneficial ownership, or through operation arrangements, such as outsourcing arrangements.

The Register is used by the government to prioritise and inform risk assessments to identify and manage national security risks in critical infrastructure assets. The ownership and operational information on the Register provides the government with a more comprehensive understanding of how the asset and sector operates, and where there may be vulnerabilities. The information on the Register also influences the government's ability to develop strategies to mitigate or reduce national security risk for assets which, if disrupted, would significantly impact the operations of large population hubs, economic interests and government operations.

The information on the Register may be shared with the relevant states and territories. This information may have broader policy implications for states and territories, particularly in relation to maintaining the security and resilience of critical infrastructure assets vital for their jurisdiction. This acknowledges that the states and territories, as owners and regulators of critical infrastructure assets share the responsibility with the government to manage national security risk. While states and territories usually do not own or operate critical telecommunications assets, these assets and their interdependencies are critical to ensuring the ongoing function of assets owned and regulated by state and territory governments. Further, some state-owned or regulated assets may incidentally be critical telecommunications assets because they hold a carrier licence. In either circumstance, information will only be shared when absolutely necessary.

Obligation to notify of cyber security incidents

Cyber security incidents may include incidents that had, or are having, a significant impact (whether direct or indirect) on the availability of an asset; and incidents that had, are having, or are likely to have, a relevant impact (defined in section 8G of the SOCI Act) on the asset. The 'switching on' of the obligation for responsible entities of critical telecommunications assets (carriers and relevant CSP assets) to report cyber incidents to the ACSC may involve the disclosure of personal information of personnel.

Government requires knowledge about cyber security incidents to enable rapid incident response, consequence management and to support the recovery of victim entities. Beyond the immediate event, knowledge of cyber security incidents allows the ACSC to increase their understanding of the threat environment and feed this intelligence back to critical infrastructure owners and operators to improve awareness of the threat environment in industry and government.

Authorised Version Explanatory Statement registered 13/03/2025 to F2025L00324

To the extent that information provided in requirement with the obligation to notify of cyber security incidents may involve personal information, this will be to enable the ACSC to assist the victim entity to respond to a cyber-incident and manage the consequences. If personal information is disclosed more broadly by the ACSC, it would be to law enforcement or security agencies for the purpose of responding to the cyber security incident.

Personal information relating to cyber incident response may involve the identity and contact details of the Chief Information Security Officer for a critical infrastructure entity or other key contacts who are best placed to assist agencies respond to an incident. Only information that is strictly required will be collected or disclosed.

Protections

The government has taken sufficient steps to ensure that any engagement with the right to privacy is no more restrictive than necessary by ensuring that any collection and disclosure of personal information as a result of the amendments to the Application Rules is restricted to purposes authorised under the SOCI Act. All information obtained under the SOCI Act, including information obtained for the Register and as a result of reporting a cyber-security incident, is protected information. It is a criminal offence to use or disclose protected information other than as authorised by Part 4, Division 3 of the SOCI Act. This Division enables disclosure for national security, foreign investment in Australia, taxation policy, industry policy, defence purposes or to assist regulatory bodies with oversight of any relevant industry for the critical infrastructure asset. 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 information provided for in the Australian Privacy Principles (APP) in Schedule 1 to the *Privacy Act 1988* will apply to information regarding interest and control, as well as operational information gathered under Part 2, and Part 2B of the SOCI Act. This includes requirements regarding the security of personal information specified under APP 11 and restrictions regarding use or disclosure of personal information under APP 6.

To the extent that the amendments to the Application Rules may result in the collection and disclosure of personal information and engage the right to privacy, any limitation is permissible as the collection and disclosure of personal information is lawful, will not be arbitrary and will be reasonable, necessary and proportionate to achieving a legitimate national security objective.

Conclusion

This Disallowable Legislative Instrument is compatible with human rights because it promotes the protection of human rights, and to the extent that it may limit human rights, those limitations are not arbitrary or unlawful and are reasonable, necessary and proportionate to the legitimate objective of reducing national security risks.

The Honourable Tony Burke MP

Minister for Home Affairs

Minister for Cyber Security

Authorised Version Explanatory Statement registered 13/03/2025 to F2025L00324