Security of Critical Infrastructure (Telecommunications Security and Risk Management Program) Rules 2024

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

Dated 2024

Tony Burke **EXPOSURE DRAFT ONLY—NOT FOR SIGNATURE**
Minister for Home Affairs
Minister for Cyber Security

EXPOSURE DRAFT ONLY

Contents

Part 1—Preliminary

1 Name 1
2 Commencement 1
3 Authority 1
4 Definitions 1
5 Meaning of ***relevant critical infrastructure asset*** 3

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

6 Application of section 30EB of the ***Act*** 4

Part 3—Part 2A – Critical infrastructure risk management programs requirements

7 Application of Part 2A of the ***Act*** 4
8 Material Risk 4
9 General - All Hazard 5
10 ***Cyber and information security hazards*** 6
11 ***Personnel hazards*** 7
12 ***Supply chain hazards*** 8
13 ***Physical security hazard*** and ***natural hazards*** 9

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

14 Application provision 10
15 Notification requirements 10

EXPOSURE DRAFT ONLY

Part 1—Preliminary

1 Name

This instrument is the *Security of Critical Infrastructure (Telecommunications Security and Risk Management Program) Rules 2024*.

2 Commencement

This 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 the *Security of Critical Infrastructure and Other Legislation Amendment (Enhanced Response and Prevention) Act 2024*.

3 Authority

This instrument is made under section 61 of the *Security of Critical Infrastructure Act 2018.*

4 Definitions

Note: A number of expressions used in this instrument are defined in section 5 of the Act, including the following:

(a) business critical data;
(b) carriage service provider;
(c) carrier;
(d) computer;
(e) critical component;
(f) critical infrastructure asset
(g) critical worker;
(h) managed service provider
(i) relevant impact;
(j) responsible entity;
(k) Secretary (except for the purposes of section 11)
(l) security.

In this instrument:

Act means the *Security of Critical Infrastructure Act 2018*.

AusCheck Act means the *AusCheck Act 2007*.

AusCheck Regulations means the *AusCheck Regulations 2017*.

background check has the same meaning as in the AusCheck Act.

broadband services means one or more services connected by means of a:

(a) fibre to building connection;
(b) fibre to the curb connection;
(c) fibre to the premises connection;

EXPOSURE DRAFT ONLY

(d) fixed wireless internet connection;
(e) hybrid fibre coaxial connection;
(f) fixed line services;
(g) satellite connection; or
(h) any other connection type.

CIRMP means critical infrastructure risk management program.

CIRMP criminal record has the same meaning as in the AusCheck Regulations.

communications has the same meaning as in the *Telecommunications Act 1997*.

criminal history criteria means the assessment of:
(a) whether the person has a CIRMP criminal record; and
(b) the nature of the offence.

cyber and information security hazard includes where a person, whether authorised or not:
(a) improperly accesses or misuses information or computer systems about, or related to, the relevant CI asset; or
(b) uses a computer system to obtain unauthorised control of, or access to, the relevant CI asset, where that control or access may impair its proper functioning.

major supplier means any vendor that, by nature of the product or service they offer, has a significant influence over the security of a responsible entity's critical telecommunications asset.

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

network-to-network interface means the physical or virtual point of connection or interconnection between a critical telecommunications asset and:
(a) another critical telecommunications asset; or
(b) a computer;
that is owned or operated by a seperate entity.

personnel hazard includes where a critical worker acts, through malice or negligence, to:
(a) compromise the proper function of the relevant CI asset; or
(b) cause significant damage to the relevant CI asset.

physical security hazard includes the unauthorised access to, interference with, or control of a relevant CI asset, that could compromise the proper function or the asset or to cause significant damage to the asset.

relevant carriage service provider asset is 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:

EXPOSURE DRAFT ONLY

(i) broadband services;
(ii) fixed telephone services;
(iii) public mobile telecommunications services;
(iv) 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).

relevant CI asset means a relevant critical infrastructure asset.

relevant critical infrastructure asset has the meaning given by section 5.

supply chain hazard includes malicious people, both internal or external, exploiting, misusing, accessing or disrupting a supply chain and over-reliance on particular suppliers.

5 Meaning of *relevant critical infrastructure asset*

For the purposes of these Rules, a ***relevant critical infrastructure asset*** is a critical telecommunications asset that is:

(a) owned or operated by a carrier; or

(b) a relevant carriage service provider asset.

Note For the critical infrastructure assets specified in section 5, a data storage system that meets all of the requirements under subsection 9(7) of the Act in respect of a critical infrastructure asset specified in section 5 is taken to be part of the critical infrastructure asset.

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

6 Application of section 30EB of the Act

For the purposes of subsection 30EB(1) of the Act, a relevant CI asset is prescribed.

Part 3—Part 2A Critical infrastructure risk management programs requirements

7 Application of Part 2A of the Act

(1) For the purposes of paragraph 30AB(1)(a) of the Act, a relevant CI asset is specified.

(2) For the purposes of subsection 30AB(3) of the Act, Part 2A of the Act does not apply to a relevant CI asset during the period beginning when the asset becomes a relevant CI asset and ending on the later of:

(a) 6 months after the commencement of this instrument; and

(b) 6 months after the asset has become a relevant CI asset.

EXPOSURE DRAFT ONLY

8 Material Risk

For the purposes of subsection 30AH(8) of the Act, material risk includes:

(a) a stoppage or major slowdown of the relevant CI asset's function for an unmanageable period;

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

(c) a substantive loss of access to, or deliberate or accidental manipulation of, a critical component of the relevant CI asset;

Example: The position, navigation and timing systems affecting provision of service or function of the relevant CI asset.

(d) an interference with the relevant CI asset's operational or information communication technology essential to the function of the asset;

Example: a billing and charging system

(e) the storage, transmission or processing of information relevant to the operation of the relevant CI asset outside of Australia, which includes:

(i) layout diagrams;

(ii) schematics;

(iii) geospatial information;

(iv) configuration information;

(v) operational constraints or tolerances information; or

(vi) data that a reasonable person would consider to be confidential; or sensitive about the asset;

(f) remote access to operational control or operational monitoring systems of the relevant CI asset;

(g) compromise, theft or manipulation of communications; or

(h) unauthorised use which compromises the security and function of a relevant CI asset, including by a:

(i) major supplier;

(ii) critical worker; or

(iii) managed service provider;

Example: software installed by a major supplier on a modem without the knowledge of the responsible entity.

(i) impact om the availability, integrity, reliability or confidentiality of the data storage system holding business critical data.

9 General—all hazards

(1) For the purpose of paragraph 30AH(1)(c) of the Act, a responsible entity must establish and maintain a process or system as part of the entity's CIRMP:

(a) to identify the operational context of the relevant CI asset;

(b) to identify the material risks, which may include those risks mentioned in section 8;

(c) as far as it is reasonably practicable to do so:

(i) to minimise or eliminate the material risks, which may include those rules mentioned in section 8; and

EXPOSURE DRAFT ONLY

(ii) to mitigate the relevant impact of each hazard on the relevant CI asset.

(d) to review the CIRMP to ensure compliance with section 30AE of the Act; and

(e) to keep the CIRMP current to ensure that it complies with section 30AF of the Act.

(2) For the purposes of subsection 30AKA(1) of the Act, a responsible entity must have regard to whether the entity's CIRMP:

(a) describes the outcome of the process or system covered by subsection (1);

(b) describes the interdependencies between the entity's relevant CI assets and other relevant CI assets;

(c) identifies each position in the entity:

(i) that is responsible for developing and implementing the CIRMP; and

(ii) for the processes mentioned in paragraph (1)(d)—that is responsible for reviewing the CIRMP or keeping the CIRMP up to date;

(d) contains the contact details for the occupant of the positions covered by paragraph 9(2)(c);

(e) contains a risk management methodology; and

(f) describes the circumstances in which the entity will review the CIRMP.

10 Cyber and information security hazards

(1) For the purpose of paragraph 30AH(1)(c) of the Act, subsections (2), (3) and (4) specify the requirements for cyber and information security hazards.

(2) A responsible entity must establish and maintain a process or system in the CIRMP to, as far as it is reasonably practicable to do so:

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

(b) mitigate the relevant impact of a cyber and information security hazard on the relevant CI asset.

All relevant critical infrastructure assets

(3) A responsible entity for a relevant CI asset must establish and maintain a process or system in the CIRMP to:

(a) comply with a framework contained in a document mentioned in the following table as in force from time to time;

(b) meet any conditions mentioned in the table for the document within 12 months after the end of the applicable period mentioned in subsection 7(2).

Item	Document	Condition
1	Australian Standard AS ISO/IEC 27001:2015	
2	Essential Eight Maturity Model published by the Australian Signals Directorate	Meet maturity level one as indicated in the document

EXPOSURE DRAFT ONLY

3	Framework for Improving Critical Infrastructure Cybersecurity published by the National Institute of Standards and Technology of the United States of America	
4	Cybersecurity Capability Maturity Model published by the Department of Energy of the United States of America	Meet maturity level one as indicated in the document
5	The 2020-21 AESCSF Framework Core published by Australian Energy Market Operator Limited (ACN 072 010 327)	Meet security profile one as indicated in the document

Note Sections 30AN and 30ANA of the Act provide for the incorporation of the documents mentioned in this subsection as in force from time to time.

Assets owned or operated by carriers

(4) A responsible entity for a critical telecommunications asset that is owned or operated by a carrier must establish and maintain a process or system in the CIRMP to:

(a) comply with a framework contained in a document mentioned in the following table as in force from time to time;

(b) meet any conditions mentioned in the table for the document within 24 months after the end of the applicable period mentioned in subsection 7(2).

Item	Document	Condition
1	Essential Eight Maturity Model published by the Australian Signals Directorate	Meet maturity level two as indicated in the document
2	Cybersecurity Capability Maturity Model published by the Department of Energy of the United States of America	Meet maturity level two as indicated in the document
3	The 2020-21 AESCSF Framework Core published by Australian Energy Market Operator Limited (ACN 072 010 327)	Meet security profile two as indicated in the document

Note Sections 30AN and 30ANA of the Act provide for the incorporation of the documents mentioned in this subsection as in force from time to time.

(5) A responsible entity for an asset mentioned in subsection (3) or (4) must establish and maintain a process or system in the entity's CIRMP to comply with a framework that is equivalent to a framework in a document mentioned in the tables including any conditions.

11 Personnel hazards

(1) For the purposes of paragraph 30AH(1)(c) of the Act, for a personnel hazard, a responsible entity must establish and maintain a process or system in the entity's CIRMP:

(a) to identify the entity's critical workers; and

EXPOSURE DRAFT ONLY

(b) to permit a critical worker access to critical components of the relevant CI asset only where the critical worker has been assessed to be suitable to have such access; and

(c) as far as it is reasonably practicable to do so—to minimise or eliminate the material risks:

(a) arising from malicious or negligent employees or contractors; and

(b) arising from the off-boarding process for outgoing employees and contractors.

(2) For purpose of paragraphs 30AH(1)(b) and (4)(a) of the Act, the process or systems for assessing the suitability of a critical worker may be a background check conducted under the AusCheck scheme.

Note Responsible entities are not required to use the AusCheck scheme to assess the suitability of critical workers. It is open for responsible entities to use other measures to assess the suitability of critical workers. That process or system must be included in the CIRMP.

(3) If a CIRMP permits a background check to be conducted under subsection (2), the background check must include an assessment of information relating to the matters mentioned in:

(a) paragraphs 5(a) to (d) of the AusCheck Act;

(b) paragraph 30AH(4)(c) of the Act with regard to the criteria against which the information must be assessed are the criminal history criteria; and

(c) paragraph 30AH(4)(d) of the Act with regard to the assessment must consist of both an electronic identity verification check and an in person identity verification check.

(4) A responsible entity must notify the Secretary if a background check is no longer required for a critical worker.

(5) In making a suitability assessment mentioned in paragraph (1)(b), a responsible entity must consider the following:

(a) any advice from the Secretary under the following provisions of the AusCheck Regulations:

(i) paragraph 21DA(2)(a);

(ii) paragraph 21DA(2)(b);

(iii) subsection 21DA(4); and

(iv) subsection 21DA(5);

(b) whether permitting a critical worker to have access to critical components of the relevant CI asset would be prejudicial to security; and

(c) any other information that may affect the person's suitability to have access to the critical components of the relevant CI asset.

Note: 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 – see AusCheck Regulations section 21ZA.

(6) For the purposes of subsections 30AKA(1), (3) and (5) of the Act, a responsible entity must have regard:

(a) to whether the CIRMP lists the entity's critical workers; and

(b) to whether the CIRMP describes the personnel risks, the occurrence of which could have a relevant impact on the asset.

(7) In this section, ***Secretary*** has the same meaning as in subsection 4(1) of the AusCheck Act.

12 Supply chain hazards

(1) For the purpose of paragraph 30AH(1)(c) of the Act, for supply chain hazards, a responsible entity must establish and maintain in the entity's CIRMP, a process or system to:

(a) as far as it is reasonably practicable to do so – minimise or eliminate the following material risks:

(i) unauthorised access, interference or exploitation of the asset's supply chain;

(ii) misuse of privileged access to the asset by any provider in the supply chain;

(iii) disruption of the asset due to an issue in the supply chain;

(iv) arising from threats to people, assets, equipment, products, services, distribution and intellectual property within supply chains;

(v) arising from major suppliers; and

(vi) any failure or lowered capacity of other assets and entities in the entity's supply chain;

(b) as far as it is reasonably practicable to do so – mitigate the relevant impact of a supply chain hazard on the asset.

(2) For the purpose of subsection 30AKA(1), (3) and (5) of the Act, a responsible entity must have regard to whether:

(a) the CIRMP lists the entity's major suppliers; and

(b) the CIRMP describes the supply chain hazards that could have a relevant impact on the asset.

13 Physical security hazards and natural hazards

(1) For the purposes of paragraph 30AH(1)(c) of the Act, for physical security hazards and natural hazards, a responsible entity must establish and maintain a process or system in the entity's CIRMP:

(a) to identify the physical critical components of the relevant CI asset; and

(b) as far as is it reasonably practicable to do so—to minimise or eliminate a material risk and mitigate a relevant impact, of:

(i) a physical security hazard on a physical critical component; and

(ii) a natural hazard to the relevant CI asset; and

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

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

EXPOSURE DRAFT ONLY

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

(2) For the purposes of subsections 30AKA(1), (3) and (5) of the Act, a responsible entity must have regard to whether:

(a) the asset's critical components are described in the CIRMP; and

(b) the physical security hazards, the occurrence of which could have a relevant impact on a physical critical components, are described in the CIRMP; and

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

(d) the CIRMP describes the natural hazards, the occurrence of which could have a relevant impact on the physical critical component.

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

14 Application provision

For the purposes of subsection 30EC(1) of the Act, a critical telecommunications asset that is owned or operated by a carrier is prescribed.

15 Notification requirements

(1) For the purposes of paragraph 30EC(2)(d) of the Act, a responsible entity must provide all information that is reasonably necessary for the Secretary to make an assessment of the change or proposed change.

(2) Without limiting subsection (1), and for the purposes of paragraph 30EC(2)(d) of the Act, the responsible entity must, as far as it is reasonably practicable to do so, provide to the Secretary:

(a) a risk assessment of the change or proposed change which considers (where relevant):

(i) material risks;

(ii) supply chain hazards;

(iii) physical security and natural hazards;

(iv) personnel hazards;

(v) cyber and information hazards;

(b) written evidence that the responsible entity has:

(i) evaluated how controls could minimise or eliminate hazards or materials risks identified in paragraph (2)(a); and

(ii) assessed the material risks of other changes that could achieve the intended project outcome.

(c) details on all software and hardware that are introduced, utilised, changed or affected, including but not limited to:

(i) version numbers for the relevant operating systems; and

(ii) other major software components.

(d) details of any major supplier relevant to the project, including any contracts or outsourcing arrangements that relate to each new:
    (i) hardware element; or
    (ii) software element; or
    (iii) third party service arrangement.
(e) detailed schematics and system documentation that describes (where relevant):
    (i) interfaces with existing elements of the critical telecommunications asset;
    (ii) security controls;
    (iii) how business critical data used in connection with any computer introduced by the proposed change is used or stored; and
    (iv) network-to-network interfaces with third party systems, including other critical telecommunications assets.
(f) a timeline of the planning, development and implementation of the proposed changes; and
(g) any other relevant information.

EXPOSURE DRAFT ONLY