LIN 23/006

Security of Critical Infrastructure (Critical infrastructure risk management program) Rules (LIN 23/006) 2023

I, Clare O'Neil, Minister for Home Affairs, make this instrument under section 61 of the *Security of Critical Infrastructure Act 2018* (the ***Act***).

Dated 31 January 2023

Clare O'Neil

Minister for Home Affairs

Part 1 Preliminary

1 Name

This instrument is the *Security of Critical Infrastructure (Critical infrastructure risk management program) Rules (LIN 23/006) 2023*.

2 Commencement

This instrument commences on the later of:

(a) immediately after the *AusCheck Legislation Amendment (Critical Infrastructure Background Check) Regulations 2023* commence; and

(b) the day after registration.

3 Definitions

Note A number of phrases used in this instrument are defined in the Act, including:

(a) critical component;

(b) critical infrastructure asset;

(c) critical hospital;

(d) critical worker;

(d) relevant impact;

(e) responsible entity;

(f) security.

In this instrument:

AusCheck Act means the *AusCheck Act 2007*.

AusCheck Regulations means the *AusCheck Regulations 2017*.

background check means a background check under the AusCheck Act.

CI asset means a critical infrastructure asset.

CIRMP is short for critical infrastructure risk management program.

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

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 CI asset; or

(b) uses a computer system to obtain unauthorised control of, or access to the CI asset that might impair its proper functioning.

designated hospital means a critical hospital mentioned in Schedule 1.

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 CI asset.

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

personnel hazard includes where a critical worker acts, through malice or negligence:

(a) to compromise the proper function of the asset; or

(b) to cause significant damage to the asset.

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

Secretary has the same meaning as defined in the AusCheck Act.

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

4 Application of Part 2A of the Act

(1) For paragraph 30AB(1)(a) of the Act, each of the following is specified:

(a) a critical broadcasting asset;

(b) a critical domain name system;

(c) a critical data storage or processing asset;

(d) a critical electricity asset;

(e) a critical energy market operator asset;

(f) a critical gas asset;

(g) a designated hospital;

(h) a critical food and grocery asset;

(i) a critical freight infrastructure asset;

(j) a critical freight services asset;

(k) a critical liquid fuel asset;

(l) a critical financial market infrastructure asset mentioned in paragraph 12D(1)(i) of the Act;

(m) a critical water asset.

(2) For subsection 30AB(3) of the Act, Part 2A of the Act does not apply to a CI asset mentioned in subsection 4(1) during the period beginning when the asset became a CI asset and ending the later of:

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

(b) 6 months after the asset became a CI asset.

(3) The requirements specified in this instrument for paragraph 30AH(1)(c), and subsections 30AKA(1), (3) and (5) of the Act, apply to a CI asset:

(a) that is:

(i) specified in subsection 4(1); and

(ii) not specified in another instrument for paragraph 30AB(1)(a) of the Act; or

(b) referred to in paragraph 30AB(1)(b) of the Act.

5 Relevant Commonwealth regulator

For subparagraph (b)(ii) of the definition of ***relevant Commonwealth regulator*** in section 5 of the Act, the Reserve Bank of Australia is specified for a critical financial market infrastructure asset mentioned in paragraph 12D(1)(i) of the Act.

Part 2 Requirements for a critical infrastructure risk management program

6 Material risk

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

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

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

Example The position, navigation and timing systems affecting provision of service or functioning of the asset.

(c) an interference with the CI asset's operational technology or information communication technology essential to the functioning of the asset;

Example A Supervisory Control and Data Acquisition (SCADA) system.

(d) the storage, transmission or processing of sensitive operational information outside Australia, which includes:

(i) layout diagrams;
(ii) schematics;
(iii) geospatial information;
(iv) configuration information;
(v) operational constraints or tolerances information;
(vi) data that a reasonable person would consider to be confidential or sensitive about the asset;

(e) remote access to operational control or operational monitoring systems of the CI asset.

7 General—all hazards

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

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

(b) to identify the material risks to the CI asset; and

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

(i) to minimise or eliminate the material risks, which may include those mentioned in section 6; and
(ii) to mitigate the relevant impact of each hazard on the CI asset; and

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

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

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

(a) describes the outcome of the process or system mentioned in paragraph (1)(a);

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

(c) identifies each position within 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 positions described under paragraph (c);

(e) contains a risk management methodology;

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

8 Cyber and information security hazards

(1) For paragraph 30AH(1)(c) of the Act, subsections (2) and (3) specify 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 CI asset.

(3) Within 12 months after the end of the applicable period mentioned in subsection 4(2), a responsible entity must comply with subsection (4) or (5).

(4) A responsible entity 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; and

(b) meet any conditions mentioned in the table for the document.

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
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 Indicator Level 1 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 1 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 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 subsection (4), including any conditions.

(6) For subsections 30AKA(1), (3) and (5) of the Act, a responsible entity must have regard to whether the entity's CIRMP describes the cyber and information security hazards that could have a relevant impact on the asset.

9 Personnel hazards

(1) For paragraph 30AH(1)(c) of the Act, for personnel hazards, 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

(b) to permit a critical worker access to critical components of the 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 following material risks:

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

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

(2) For paragraph (1)(b) and paragraph 30AH(4)(a) of the Act, the process or system 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 assessment of information relating to the matters mentioned in paragraphs 5(a), (b), (c) and (d) of the AusCheck Act; and

(a) for paragraph 30AH(4)(c) of the Act—the criteria against which the information must be assessed are the criminal history criteria; and

(b) for paragraph 30AH(4)(d) of the Act—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);

(iv) subsection 21DA(5); and

(b) whether permitting a critical worker to have access to critical components of the 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 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 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.

10 Supply chain hazards

(1) For 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; and

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

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

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

(v) arising from major suppliers; and

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

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

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

(b) to whether the CIRMP describes the supply chain hazards, which could have a relevant impact on the asset.

11 Physical security hazards and natural hazards

(1) For 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 CI asset; and

(b) as far as it is 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 on the 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

(e) to 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.

(2) For 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 component, 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.

Schedule 1 Designated hospitals

(section 3)

A designated hospital means a critical hospital mentioned in an item in the following table located in the State or Territory mentioned in the item.

Item	Hospital	State or Territory
1	Bankstown-Lidcombe Hospital	New South Wales
	Blacktown Hospital	
	Calvary Mater Newcastle	
	Campbelltown Hospital	
	Children's Hospital Westmead	
	Coffs Harbour Health Campus	
	Concord Repatriation General Hospital	
	Dubbo Base Hospital	
	Gosford Hospital	
	Hornsby Ku-Ring-Gai Hospital	
	John Hunter Hospital	
	Lake Macquarie Private Hospital	
	Lismore Base Hospital	
	Liverpool Hospital	
	Nepean Hospital	
	Northern Beaches Hospital	
	Northern Beaches Hospital	
	Orange Base Hospital	
	Port Macquarie Base Hospital	
	Prince of Wales Hospital	
	Royal North Shore Hospital	
	Royal Prince Alfred Hospital	
	St George Hospital	
	St Vincent's Hospital (Darlinghurst)	
	Sydney Children's Hospital	
	Tamworth Hospital	
	The Sutherland Hospital	
	The Tweed Hospital	
	Wagga Wagga Base Hospital	
	Westmead Hospital	
	Wollongong Hospital	
2	Austin Hospital – Austin Health	Victoria
	Box Hill Hospital – Eastern Health	
	Cabrini Malvern	
	Dandenong Hospital – Monash Health	
	Frankston Hospital – Peninsula Health	
	Knox Private Hospital	
	Monash Children’s Hospital – Monash Health	
	Monash Medical Centre (Clayton) – Monash Health	
	Northern Hospital – Northern Health	
	Royal Melbourne Hospital – Melbourne Health	

Item	Hospital	State or Territory
	St Vincent's Hospital (Melbourne) Limited	
	The Alfred – Alfred Health	
	The Royal Children's Hospital	
	The Royal Women's Hospital	
	University Hospital (Geelong) – Barwon Health	
3	Bundaberg Base Hospital	Queensland
	Caboolture Hospital	
	Cairns Base Hospital	
	Gold Coast University Hospital	
	Greenslopes Private Hospital	
	Hervey Bay Hospital	
	Ipswich Hospital	
	Logan Hospital	
	Mackay Base Hospital	
	Mater Adult Hospital	
	Mater Hospital Brisbane	
	Princess Alexandra Hospital	
	Queen Elizabeth II Jubilee Hospital	
	Queensland Children's Hospital	
	Redcliffe Hospital	
	Robina Hospital	
	Rockhampton Hospital	
	Royal Brisbane & Women's Hospital	
	Sunshine Coast Public University Hospital	
	The Prince Charles Hospital	
	The Wesley Hospital	
	Toowoomba Hospital	
	Townsville University Hospital	
4	Armadale Hospital	Western Australia
	Bunbury Regional Hospital	
	Fiona Stanley Hospital	
	Hollywood Private Hospital	
	Joondalup Health Campus	
	Joondalup Health Campus	
	King Edward Memorial Hospital	
	Perth's Children's Hospital	
	Rockingham General Hospital	
	Royal Perth Hospital	
	Sir Charles Gairdner Hospital	
	St John of God Midland Public Hospital	
5	Calvary Hospital Adelaide	South Australia
	Flinders Medical Centre	
	Lyell McEwin Hospital	
	Royal Adelaide Hospital	
	The Queen Elizabeth Hospital	

Item	Hospital	State or Territory
	Women's and Children's Hospital	
6	Launceston General Hospital Royal Hobart Hospital	Tasmania
7	Canberra Hospital	Australian Capital Territory
8	Alice Springs Hospital Royal Darwin Hospital	Northern Territory