LIN 22/018

Security of Critical Infrastructure (Critical infrastructure risk management program) Rules (LIN 22/018) 2022

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 2022

DRAFT ONLY—NOT FOR SIGNATURE

Minister for Home Affairs

Contents

Part 1 Preliminary

1 Name

This instrument is the *Security of Critical Infrastructure (Critical infrastructure risk management program) Rules (LIN 22/018) 2022*.

2 Commencement

This instrument commences on the day after registration.

Note The Minister can only make this instrument after the requirements mentioned in section 30AL of the Act are completed.

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 worker;

(d) material risk;

(e) relevant impact;

(f) responsible entity.

In this instrument:

asset means a critical infrastructure asset.

criminal history criteria means the assessment of:

(a) whether a person has been convicted of an offence mentioned in item 1 of Schedule 1; and

(b) whether a person has been convicted of, and sentenced to imprisonment for, an offence mentioned in item 2 of Schedule 1; and

(c) the nature of the offence.

cyber and information security hazard includes where a person, whether authorised or not, improperly accesses or misuses information or computer systems about or related to the asset, or where such person by use of a computer system obtains unauthorised control of or access to any function which may impair the proper functioning of the asset.

entity means the responsible entity for a Part 2A asset.

high risk vendor means any vendor that by nature of the product or service they offer, has a significant influence over the security of an entity's system.

natural hazard includes a bushfire, flood, cyclone, storm, heatwave, earthquake, tsunami or health hazard (such as a pandemic).

Part 2A asset means a critical infrastructure asset to which Part 2A of the Act applies, other than an asset mentioned in subsection 5(1) of *the Security of Critical Infrastructure (Naval shipbuilding) Rules (LIN 22/055) 2022* .

Part 2A critical hospital means a hospital mentioned in Schedule 2.

personnel hazard includes where a critical worker acts, through malice or negligence, to compromise the proper function of the asset or cause significant damage to the asset, as assessed by the entity, such as by causing a material risk to the asset.

physical security hazard includes the unauthorised access, interference, or control of critical assets, other than those covered by cyber and information security hazards, including where persons other than critical workers act, through malice or negligence, to compromise the proper function of the asset or cause significant damage to the asset, as assessed by the entity.

program means a critical infrastructure risk management program.

sensitive operational information includes any of the following for a Part 2A asset:

(a) layout diagrams;

(b) schematics;

(c) geospatial information;

(d) configuration information;

(e) operational constraints or tolerances information;

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

4 Application of Part 2A of the Act

(1) For paragraph 30AB(1)(a) of the Act, each of the following assets 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 Part 2A critical 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 that is a payment system;

(m) a critical water asset.

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

(a) for an asset that was a critical infrastructure asset immediately before the commencement of section 30AB of the Act—ending 6 months after the commencement of this instrument; and

(b) for any other critical infrastructure asset—ending 6 months after the asset became a critical infrastructure asset.

5 Material risk

For subsection 30AH(8) of the Act, material risks for an asset are taken to include a risk of the following relevant impacts occurring:

(a) an impairment of the asset that may prejudice the social or economic stability of Australia or its people, the defence of Australia or national security;

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

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

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

(d) an interference with the asset's operation technology or information communication technology essential to the functioning of the asset;

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

(e) an impact resulting from the storage, transmission or processing of sensitive operational information outside Australia;

(f) an impact resulting from remote access to operational control or operational monitoring systems of the asset;

(g) any other material risks as identified by the entity that affect the functioning of the asset.

6 Relevant Commonwealth regulator—payment systems

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 referred to in paragraph 12D(1)(i) of the Act.

Part 2 Requirements for a critical infrastructure risk management program

7 General

(1) For paragraph 30AH(1)(c) of the Act, an entity must establish and maintain in the entity's program:

(a) a process or system for identifying the operational context of each Part 2A asset for which the entity is responsible; and

(b) a principles-based risk identification process that the entity used to identify risks to the entity's Part 2A asset; and

(c) a risk management process or system that includes, for each material risk mentioned in section 5, a process or system to:

(i) consider the risk; and

(ii) as far as it is reasonably practicable to do so—minimise or eliminate the risk; and

(d) a process:

(i) for reviewing the program so that it complies with section 30AE of the Act; and

(ii) for keeping the program up to date so that it complies with section 30AF of the Act.

(2) In this subsection:

(a) for subsection 30AKA(1) of the Act—in deciding whether to adopt a program; and

(b) for subsection 30AKA(3) of the Act—in reviewing the program in accordance with section 30AE; and

(c) for subsection 30AKA(5) of the Act—in deciding whether to vary the program

an entity must have regard to the following matters:

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

(e) whether the program describes interdependencies between each of the entity's Part 2A assets and other critical infrastructure assets;

(f) whether the program identifies each position within the entity:

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

(ii) for each minimisation or elimination mentioned in subparagraph (1)(c)(ii)—that is responsible for developing and implementing the minimisation or elimination; and

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

(g) whether the program contains the contact details for the positions described under paragraph (f);

(h) whether the program contains a risk management methodology or principles of a reasonable risk management methodology;

(i) whether the program describes the circumstances in which the entity will review the program (even if not required by section 30AE of the Act).

8 Cyber and information security hazards

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

(2) The entity must establish and maintain a process or system in the entity's program:

(a) to minimise or eliminate a material risk that a cyber and information security hazard for which there is a material risk that the hazard could have a relevant impact on the asset; and

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

(3) Within 12 months of Part 2A of the Act applying to an asset, an entity must comply with either subsection (4) or (5).

Note See also subsection 4(2) and section 30AB of the Act.

(4) To comply with this subsection, the entity must:

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

(b) if a condition is mentioned in the item—comply with the condition.

Item	Document	Condition
1	Australian Standard *AS ISO/IEC 27001:2015*	
2	*Essential Eight Maturity Model* published by the Australian Signals Directorate	Required to 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	Required to 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)	Required to 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) To comply with this subsection, the entity must comply with a framework that is equivalent to a framework in a document mentioned in subsection (4), including a condition (if any) mentioned for that document.

(6) In this subsection:

(a) for subsection 30AKA(1) of the Act—in deciding whether to adopt a program; and

(b) for subsection 30AKA(3) of the Act—in reviewing the program in accordance with section 30AE; and

(c) for subsection 30AKA(5) of the Act—in deciding whether to vary the program

an entity must have regard to whether the cyber and information security risks, the occurrence of which could have a relevant impact on the asset, are described in the program.

9 Personnel hazards

(1) For paragraph 30AH(1)(c) of the Act, subsection (2) specifies a requirement in relation to a material risk that an occurrence of a personnel hazard could have a relevant impact on a Part 2A asset.

(2) An entity must establish and maintain a process or system in the entity's program:

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

(b) to assess, on an ongoing basis, the suitability of a critical worker to have access to the critical components of the asset; and

(c) minimise or eliminate material risks that negligent employees and malicious insiders may cause to the functioning of the asset; and

(d) minimise or eliminate material risks arising from the off-boarding process for outgoing employees and contractors.

(3) For paragraph (2)(b) and paragraph 30AH(4)(a) of the Act, the process and system for assessing the suitability of a critical worker to have access to the critical components of the asset may be a background check under the AusCheck scheme at regular intervals.

(4) For a background check of an individual permitted under subsection (3):

(a) for paragraph 30AH(4)(b) of the Act—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 2007*; and

(b) for paragraph 30AH(4)(c) of the Act, if the background check includes an assessment of information relating to the matter mentioned in paragraph 5(a) of the *AusCheck Act 2007*—the criteria against which the information must be assessed are the criminal history criteria; and

(c) for paragraph 30AH(4)(d) of the Act, if the background check includes an assessment of information relating to the matter mentioned in paragraph 5(d) of the *AusCheck Act 2007*—the assessment must consist of both an electronic identity verification check and an in person identity verification check.

Note In this exposure draft, subsections (3) and (4) are included to indicate how background checks under the AusCheck scheme will be enabled. The specific operation of the AusCheck scheme, including the associated amendments required for the *AusCheck Regulations 2017* to enable such background checks, will be the subject of further consultation before being finalised.

(5) In this subsection:

(a) for subsection 30AKA(1) of the Act—in deciding whether to adopt a program; and

(b) for subsection 30AKA(3) of the Act—in reviewing the program in accordance with section 30AE; and

(c) for subsection 30AKA(5) of the Act—in deciding whether to vary the program

an entity must have regard to:

(d) whether the program lists the entity's critical workers; and

(e) whether the personnel risks, the occurrence of which could have a relevant impact on the asset, are described in the program.

10 Supply chain

(1) Subsection (2) specifies a requirement for paragraph 30AH(1)(c) of the Act.

(2) An entity must establish and maintain in the entity's program a process or system that the entity uses to minimise or eliminate the material risk of, or mitigate, the relevant impact of:

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

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

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

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

(e) high risk vendors; and

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

11 Physical security hazards and natural hazards

(1) Subsection (2) specifies a requirement for paragraph 30AH(1)(c) of the Act.

(2) An entity must establish and maintain a process or system in the entity's program:

(a) to identify the parts of the asset that are critical to the functioning of the asset (the ***critical sites***); and

(b) to minimise or eliminate a material risk of, or mitigate, a relevant impact of a physical security hazard on a critical site; and

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

(d) to control access to critical sites, 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; and

(f) to minimise or eliminate a material risk of, or mitigate, a relevant impact of a natural hazard on the asset.

(3) In this subsection:

(a) for subsection 30AKA(1) of the Act—in deciding whether to adopt a program; and

(b) for subsection 30AKA(3) of the Act—in reviewing the program in accordance with section 30AE; and

(c) for subsection 30AKA(5) of the Act—in deciding whether to vary the program

an entity must have regard to:

(d) whether the asset's critical sites are described in the program;

(e) whether the physical security hazards, the occurrence of which could have a relevant impact on a critical site, are described in the program;

(f) whether the security arrangements for the asset are described in the program;

(g) whether the natural hazards, the occurrence of which could have a relevant impact on the asset, are described in the program.

Schedule 1 Criminal history criteria

(section 3, definition of ***criminal history criteria***)

1 Where individual has been convicted of offence

Item	Offence
1	An offence involving, or relating to, a weapon of mass destruction
2	An offence involving, or relating to, terrorism
3	An offence involving, or relating to, any of the following: (a) treason; (b) espionage; (c) disclosure of national secrets
4	An offence involving or relating to: (a) engagement in hostile activities in a foreign country; or (b) involvement with foreign armed forces
5	An offence involving, or relating to, the hijacking or destruction of: (a) an aircraft; or (b) a vessel; or (c) an offshore facility
6	An offence involving, or relating to, the endangerment of an aircraft, airport, vessel, port or offshore facility that is: (a) used in commerce; or (b) owned by the Commonwealth or a State or Territory
7	An offence involving, or relating to, an act of piracy at sea
8	An offence involving or relating to: (a) slavery; or (b) smuggling or trafficking of people
9	An offence involving, or relating to, a crime against humanity
10	An offence involving, or relating to, any of the following: (a) murder; (b) manslaughter; (c) threat to kill
11	An offence involving, or relating to, assault, including any of the following: (a) indecent assault; (b) sexual assault; (c) sexual abuse
12	An offence involving, or relating to, any of the following: (a) firearms; (b) ammunition; (c) weapons, including use of an item as a weapon; (d) explosives or explosive devices; (e) microbial or other biological agents or toxins
13	An offence involving or relating to: (a) destruction of, or damage to, property; (b) arson

14	An offence involving, or relating to, affray, riot or public violence
15	An offence involving, or relating to, any of the following: (a) false imprisonment; (b) deprivation of liberty; (c) kidnapping; (d) taking a hostage
16	An offence involving, or relating to, participation in, or association with, serious and organised crime or gangs
17	An offence involving, or relating to, exploitation of a child
18	An offence involving, or relating to, robbery

2 Where individual has been convicted of offence and sentenced to imprisonment

Item	Offence
1	An offence involving, or relating to, fraud, forgery, false identity or false identity documents
2	An offence involving, or relating to, any of the following: (a) perjury; (b) perverting the course of justice; (c) intimidation
3	An offence involving, or relating to, the production, possession, supply, importation or export of any of the following: (a) an illegal drug; (b) a controlled substance (within the meaning of subsection 3(1) of the *Crimes Act 1914*)
4	An offence involving, or relating to, racial hatred or racial vilification
5	An offence involving, or relating to, any of the following: (a) money laundering; (b) currency violations; (c) dealing with proceeds of crime
6	An offence involving, or relating to, bribery, corruption, extortion, racketeering or blackmail
7	An offence involving, or relating to, obstructing, hindering, resisting or impersonating: (a) a government official; or (b) a law-enforcement officer
8	An offence involving, or relating to, use, access, modification or destruction of: (a) data; or (b) electronic communications
9	An offence involving, or relating to, theft or burglary
10	An offence involving, or relating to, the intentional endangerment of persons (not including an offence mentioned in the table in clause 1)

11	An offence involving or relating to: (a) illegal importation or export of goods, fauna or flora; or (b) interference with goods under customs control

Schedule 2 Part 2A critical hospitals

(section 3)

A Part 2A critical hospital means a critical hospital located in a State or Territory mentioned in an item of the following table that is described as mentioned in the item.

Item	State or Territory	Description
1	New South Wales	*See further discussion in explanatory statement.*
2	Victoria	*See further discussion in explanatory statement.*
3	Queensland	*See further discussion in explanatory statement.*
4	Western Australia	*See further discussion in explanatory statement.*
5	South Australia	*See further discussion in explanatory statement.*
6	Tasmania	*See further discussion in explanatory statement.*
7	Australian Capital Territory	*See further discussion in explanatory statement.*
8	Northern Territory	*See further discussion in explanatory statement.*

Note In this exposure draft, the table is included to indicate that only certain critical hospitals will be required to establish and maintain a critical infrastructure risk management program under Part 2A of the Act, by operation of section 4 of the *Security of Critical Infrastructure (Critical infrastructure risk management program) Rules (LIN 22/018) 2022*. What particular descriptions will be included in the table is subject to further consultation.