EXPLANATORY STATEMENT

Issued by authority of the Minister for Home Affairs

Security of Critical Infrastructure Act 2018

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

1 The instrument, Departmental reference LIN 22/018, is made under section 61 of the *Security of Critical Infrastructure Act 2018* (the Act).

2 The instrument commences on the day after registration and is a legislative instrument for the *Legislation Act 2003* (the Legislation Act).

Purpose

3 Part 2A of the Act was inserted by the *Security Legislation Amendment (Critical Infrastructure Protection) Act 2022*, and provides that the responsible entity for one or more critical infrastructure assets must have, and comply with, a critical infrastructure risk management program unless an exemption applies.

4 The purpose of a critical infrastructure risk management program is to ensure that the responsible entity for each of those assets:

- identifies each hazard where there is a material risk that the occurrence of the hazard could have a relevant impact on the asset;
- so far as it is reasonably practicable to do so—minimises or eliminates any material risk of such a hazard occurring;
- so far as it is reasonably practicable to do so—mitigates the relevant impact of such a hazard on the asset.

5 Section 30AB of the Act provides that Part 2A of the Act applies to a critical infrastructure asset if:

- the asset is specified in the rules (paragraph (1)(a)); or
- the asset has been privately declared to be a critical infrastructure asset under section 51 of the Act and the declaration determines that Part 2A applies to the asset (paragraph (1)(b)).

6 The instrument specifies that the obligations in Part 2A of the Act are 'switched on' for the critical infrastructure assets that are specified in the instrument. The rules also provide responsible entities with a period of 6 months before they will be required to comply with obligations under Part 2A of the Act.

7 The instrument sets out the requirements, for paragraph 30AH(1)(c) of the Act, that an entity must establish and maintain in the entity's program. The instrument also sets matters that must be considered by a responsible entity when adopting, reviewing and varying their critical infrastructure risk management program for section 30AKA of the Act.

8 In specifying the requirements in the rules, and in accordance with subsection 30AH(6), the Minister had regard to:

- any existing regulatory system of the Commonwealth, a State or a Territory that imposes obligations on responsible entities (paragraph (a));
- the costs that are likely to be incurred by responsible entities in complying with the rules (paragraph (b));
- the reasonableness and proportionality of the requirements in the rules in relation to the purposes referred to in paragraph 30AH(1)(b) (paragraph (c)).
- such other matters (if any) as the Minister consider relevant (paragraph (d)).

Consultation

9 The Department of Home Affairs (the Department) engaged industry stakeholders from across sectors in a consultation process to design the rules underpinning the risk management program.

10 Section 30ABA of the Act requires that, before making or amending rules under section 30AB, the Minister must cause to be published on the Department's website a notice setting out the draft rules or amendments and inviting persons to make submissions about the proposed rules within the specified time period.

11 Under subsection 30AL(2) of the Act, the Minister must cause to be published a notice on the Department's website a draft of the proposed rules under section 30AH and invite submissions to the Minister. The Minister must also give a copy of the notice to each State and Territory First Minister. The Minister must consider any submissions received within the period specified in the notice. Subsection 30AL(3) of the Act specifies that the period of the notice must be no shorter than 28 days.

12 This exposure draft is made publically available to satisfy the consultation requirements of sections 30ABA and 30AL of the Act.

13 A regulation impact statement (RIS) is also being conducted in relation to the instrument. A draft RIS informed by extensive consultation with stakeholders has been developed to identify the regulatory impact of these reforms. The RIS weighs the regulatory costs of the RMP rules against the damage to the economy if business underinvests in security and allows breaches to occur. The RIS clearly identifies that the regulatory costs of complying with the critical infrastructure risk management program obligation, as specified in rules, is minimal when compared to the damage to the economy if businesses underinvest in security and allow breaches to occur.

14 The RIS highlights that existing regulatory frameworks and market forces are insufficient to protect critical infrastructure against all hazard threats in a consistent and coordinated manner across critical infrastructure assets. Moreover, the likely benefits of the critical infrastructure risk management program obligation will be at least (and are expected to be more than) the costs of the regulation. This is primarily because the frequency and severity of all-hazard risks for critical infrastructure assets are

growing and this increasing severity and frequency of incidents, particularly in the context of growing cybersecurity incidents, represents a risk to the whole economy.

15 Detailed economic analysis of costing figures received through the RIS indicates that the potential cost of the required security uplift would be significantly outweighed by the net benefits to the economy as a whole.

Details of the instrument

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

Parliamentary scrutiny etc.

17 The instrument is subject to disallowance under section 42 of the Legislation Act and the final explanatory statement for the instrument will contain a Statement of Compatibility with Human Rights in accordance with the *Parliamentary Scrutiny (Human Rights) Act 2011*.

18 The instrument will be made by the Minister for Home Affairs in accordance with the requirements of section 30AL.

Attachment A

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

Section 1 Name

This section provides that the name of the instrument is the *Security of Critical Infrastructure (Critical infrastructure risk management program) Rules 2022* (the instrument).

Section 2 Commencement

This section provides that the instrument commences on the day after registration on the Federal Register of Legislation.

Section 3 Definitions

This section sets out definitions of terms used in the instrument.

Section 3 includes a definition of *criminal history criteria*. This is defined as the assessment of:

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

Section 4 Application of Part 2A of the Act

Subsection 4(1) provide that Part 2A of the *Security of Critical Infrastructure Act 2018* (the Act) applies to the critical infrastructure assets specified in paragraphs 4(1)(a) to (m).

As a result of an asset of being specified in subsection 4(1), the responsible entities for those assets have an ongoing obligation to have, and comply with, a critical infrastructure risk management program (unless an exemption applies).

Subsection 4(2) outlines a 6 month period before a responsible entity must comply with the requirements under Part 2A of the Act. Under this provision, Part 2A of the Act does not apply to the critical infrastructure assets mentioned in subsection (1) as follows:

- for an asset that was a critical infrastructure asset immediately before the commencement of section 30AB of the Act—the period of time from when the asset became a critical infrastructure asset to 6 months after the commencement of this instrument; and
- for any other critical infrastructure asset (i.e. for assets that become critical infrastructure assets after the commencement of section 30AB of the Act)—the 6 month period from the time the asset became a critical infrastructure asset.

Section 5 Material risk

Section 5 of the instrument sets out that, under subsection 30AH(8) of the Act, a 'material risk' is taken to include any risk of the following impacts:

- an impairment of the asset that may prejudice the social or economic stability of Australia or its people, the defence of Australia or the national security of Australia (paragraph (a));
- any hazard that would cause the stoppage or major slowdown of the asset's functioning for an unmanageable period (paragraph (b));
- the substantive loss of access to or deliberate or accidental manipulation of a critical component of the asset (paragraph (c));
- interference with the asset's operating technology or information communication technology essential to the functioning of the asset (paragraph (d));
- the relevant impact on the asset resulting from the storage, transmission or processing of sensitive operational information outside Australia (paragraph (e)), with the term *sensitive operational information* further defined in section 3;
- the relevant impact on the asset resulting from remote access to operational control or operational monitoring systems of the asset (paragraph (f));
- any other material risks as identified by the entity that affect the functioning of the asset (paragraph (g)).

Section 6 Relevant Commonwealth regulator—payment systems

Section 6 of the instrument provides that, for subparagraph (b)(ii) of the definition of *relevant Commonwealth regulator* in section 5 of the Act, the Reserve Bank of Australia (RBA) is specified for a critical financial market infrastructure asset that is a payment system referred to in subparagraph 12D(1)(i) of the Act.

The *relevant Commonwealth regulator* is an entity that, under the SOCI Act:

- receives annual reports from responsible entities about the establishment, maintenance and operation of the entity's critical infrastructure risk management program; and
- may exercise compliance and monitoring functions under the *Regulatory Powers (Standard Provisions) Act 2014* in relation to an entity's critical infrastructure risk management program obligations.

For example, section 30AG of the Act provides that a responsible entity must provide an annual report in relation to its risk management program obligations in Part 2A of the Act. Subsection 30AG(2) of the Act provides that the entity must, within 90 days of the end of each financial year, give the report to either:

- if there is a relevant Commonwealth regulator that has functions relating to the security of those assets—the relevant Commonwealth regulator (paragraph (a)); or
- in any other case—the Secretary (paragraph (b)).

By operation of section 6 of the instrument and section 30AG of the Act, the responsible entity for a critical financial markets infrastructure asset that is a payment system will be required to provide the report to the RBA. For all other assets, the responsible Commonwealth regulator will be the Cyber and Infrastructure Security Centre within the Department of Home Affairs by operation of subsection 30AG(2) of the Act.

Relevant Commonwealth regulators will be responsible for educating and guiding entities towards best-practice security management wherever possible, and the RBA are best placed to provide this to entities that own and operate payment systems. This will include educating entities and ensuring their legislative and administrative obligations are understood; and developing and maintaining strong links with entities to promote ongoing best practice.

Part 2 Requirements for a critical infrastructure risk management program

Section 7 General

Subsection 7(1) of the instrument specifies general requirements that an entity must comply with when establishing and maintaining a critical infrastructure risk management program under paragraph 30AH(1)(c) of the Act. The requirements are that the program contains:

- a process or system for identifying the operational context of each Part 2A asset for which an entity is responsible (paragraph (a));
- a principles-based risk identification process used to identify risks to the entity's Part 2A assets (paragraph (b));
- a risk management process or system that includes, for each material risk, a process or system to consider the risk and minimise or eliminate the risk (paragraph (c));
- a process for reviewing the risk management program so that it remains compliant with the requirement to review the program in section 30AE of the Act (subparagraph (d)(i));
- a process for keeping the risk management program up to date so that it remains compliant with requirement to keep the program up to date under section 30AF of the Act (subparagraph (d)(ii)).

Subsection 7(2) of the instrument specifies that, in deciding to adopt, review or vary a risk management program, for section 30AKA of the Act an entity must have regard to the matters mentioned in paragraphs (d) to (i).

Describing outcomes and interdependencies

Paragraphs 7(2)(d) and (e) of the instrument provide that the entity must have regard to:

- whether the program describes the outcomes of the process or system under section 7(1)(a) for identifying the operational context of their Part 2A assets (paragraph (d)); and
- whether the program describes any interdependencies between their Part 2A assets critical and other critical infrastructure assets (paragraph (e)).

The purpose of paragraphs 7(2)(d) and (e) is to ensure that the program sets out the entity's process for identifying risk relating to critical infrastructure assets for which it is responsible. This includes matters such

as how the program will function on a daily basis, the kinds of relevant impacts that are most applicable to those assets, and interaction with other critical infrastructure assets.

Positions responsible for risk management

Paragraph 7(2)(f) of the instrument provides that the entity must have regard to whether the program the program identifies:

- each position within the entity that is responsible for developing and implementing the program (subparagraph (i));
- each position within the entity that is responsible for developing and implementing the minimisation, elimination or mitigation, as referred to in subparagraph 7(1)(c)(ii) of the instrument (subparagraph (ii));
- each position within the entity responsible for reviewing the program or keeping the program up to date, as referred to in paragraph 7(1)(d) of the instrument (subparagraph (iii));

Under paragraph 7(2)(g), the entity must have regard to whether the program includes contact details of the positions referred to in paragraph 7(2)(f).

The purpose of paragraphs 7(2)(f) and (g) is to ensure that details of the positions (and their contact details) responsible for developing and implementing a program, and eliminating or mitigating risks, are set out in the program.

Risk management methodology

Paragraph 7(2)(h) of the instrument provides that the entity must have regard to whether the program describes a reasonable risk management methodology or principles of a reasonable risk management methodology.

The purpose of this provision is to ensure that the program contains a risk management methodology, or principles of risk management methodology. This will be an overview of the process of risk management methodology that the entity uses. Generally it should cover how risks should be identified, the methods that should be used, the people who should be involved and other methodological issues.

Review of the program

Paragraph 7(2)(i) of the instrument provides that the entity must have regard to whether the program describes the circumstances in which the entity will review the program (even if not required to do so by section 30AE of the Act). Section 30AE of the Act requires a responsible entity for a critical infrastructure asset to review its program on a regular basis.

The purpose of paragraph 7(2)(i) is to ensure that the program describes how the entity will regularly review its program in accordance with section 30AE of the Act.

Section 8 Cyber and information security

Section 8 of the instrument sets out the cyber and information security hazard requirements that an entity's risk management program must comply with under the Act.

Subsection 8(1) provides that subsections (2) and (3) specify requirements for paragraph 30AH(1)(c) of the Act.

Subsection 8(2) requires that the entity must establish and maintain a process or system in the entity's critical infrastructure risk management program:

- to minimise or eliminate a material risk of a hazard that could have a relevant impact on the cyber and information security of the asset (paragraph (a)); and
- to mitigate the relevant impact of a hazard on the cyber and information security of the asset (paragraph (b)).

The purpose of subsection 8(2) is to require an entity's program to have the required level of preparedness to mitigate cyber security threats to their critical infrastructure assets.

Subsection 8(3) provides that, within 12 months of Part 2A applying to an entity, an entity must comply with *either* subsection 8(4) or 8(5). Entities are not required to comply with *both* subsections 8(4) and 8(5). This means, an entity has a further 12 months to comply with the requirements in subsection8(4) or (5), from the date prescribed in subsection 4(2).

Paragraph 8(4)(a) of the instrument requires that the entity's program must comply with one of the frameworks contained in the documents as listed in the table as in force from time to time. Paragraph 8(4)(b) requires that if there is a condition mentioned in the item associated with the document, the entity must also comply with the condition. The documents listed in the table are as follows:

- Australian Standard *AS ISO/IEC 27001:2015* (item 1);
- the *Essential Eight Maturity Model*, published by the Australian Signals Directorate, with the condition that the entity is required to meet maturity level one (item 2);
- *Framework for Improving Critical Infrastructure Cybersecurity* published by the National Institute of Standards and Technology of the United States of America (item 3);
- *Cybersecurity Capability Maturity Model* published by the Department of Energy of the United States of America, with the condition that the entity is required to meet Maturity Indicator Level 1 (item 4); and
- *The 2020-21 AESCSF Framework Core* published by Australian Energy Market Operator Limited (ACN 072 010 327), with the requirement that the entity is required to meet Security Profile 1 (item 5).

A note to this provision indicates that:

- the document listed in item 1 of the table, as an Australian Standard, can be incorporated as in force from time to time as provided for in subsection 30AN(3) of the Act; and
- the other documents (items 2-5) are defined to be 'relevant documents' in subsection 30ANA(2) of the Act, and therefore can be incorporated as in force from time to time as provided for in subsection 30ANA(1).

Under subsection 8(5), an entity must alternatively comply with a framework that is equivalent to a framework mentioned in a document mentioned in subsection 8(4). The purpose of this provision is to provide industry with the necessary flexibility to comply with their statutory obligations by recognising alternative cyber security frameworks that achieve the desired uplift in security and resilience of the entity's Part 2A asset.

Subsection 8(6) sets out matters an entity must have regard to when adopting, reviewing or varying a critical infrastructure risk management program for section 30AKA of the Act. Under this provision, the 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. 'Cyber and information security risk' is defined in section 3 of the instrument.

Section 9 Personnel hazards

Subsection 9(1) of the instrument provides that subsection 9(2) specifies the personnel hazard requirements that a critical infrastructure risk management program must comply with under paragraph 30AH(1)(c) of the Act.

Subsection 9(2) provides that an entity must establish and maintain a process or system in the entity's program:

- to identify the entity's critical workers (paragraph (a)). *Critical worker* is defined in section 5 of the Act;

- to assess, on an ongoing basis, the suitability of a critical worker to have access to the critical components of the asset (paragraph (b)). *Critical component* is defined in section 5 of the Act;

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

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

Subsection 9(3) provides that the process or system for considering the suitability of a critical worker to have access to critical components of an asset may be a background check under the AusCheck scheme.

Subsection 9(4) provides requirements for a background check of a critical worker under subsection 9(3). The requirements are that the background check must:

- provide that such a background check must include assessment of information relating to one or more of the matters mentioned in paragraphs 5(a), (b), (c) or (d) of the *AusCheck Act 2007* (AusCheck Act)—relating respectively to a criminal history check, an ASIO security assessment, an immigration status check and an identity check (paragraph (a));

- provide that if a background check includes a criminal history check pursuant to paragraph 5(a) of the AusCheck Act—the check must be assessed against the *criminal history criteria* in Schedule 1 (paragraph (b)); and

- if the background check includes an identity check pursuant to paragraph 5(d) of the AusCheck Act—provide for how that check will be conducted as an electronic identity verification check and in person identity verification check(paragraph (c)).

A note to this provision for the purpose of the exposure draft indicates that subsections (3) and (4) have been included in the instrument 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.

Subsection 9(5) sets out the matters an entity must have regard to when adopting, reviewing or varying a critical infrastructure risk management program for section 30AKA of the Act.

Under this provision, the entity must have regard to:

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

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

Section 10 Supply chain

Section 10 sets out the supply chain hazard requirements that an entity's critical infrastructure risk management program must comply with under paragraph 30AH(1)(c) of the Act (see subsection (1)).

Subsection 10(2) provides that an entity must establish and maintain in its program a process or system used to minimise or eliminate the material risk of, or mitigate, the relevant impact of:

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

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

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

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

- high risk vendors (paragraph (e)). A high risk vendor is any vendor that by nature of the product or service they offer, has a significant influence over the security of an entity's system. For example, the vendor may be subject to adverse extrajudicial direction, the vendor's poor cyber security posture may mean they are subject to adverse external interference, or the vendor may in some other way transfer unreasonable risk to an entity's system; and

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

The purpose of subsection 10(2) is to ensure that an entity's program contains necessary detail regarding the steps they are taking to secure the supply chains necessary for the operational continuity of their critical

infrastructure asset, as well as the practices they are implementing to continually monitor and enhance their supply chain security.

Section 11 Physical security hazards and natural hazards

Section 11 of the instrument sets out the physical and natural hazard requirements that an entity's critical infrastructure risk management program must comply with under paragraph 30AH(1)(c) of the Act (see subsection (1)).

Subsection 11(2) provides that an entity must establish and maintain a process or system in the entity's program:

- to identify the parts of the asset that are critical to the functioning of the asset (the *critical sites*) (paragraph (a)); and
- to minimise or eliminate a material risk of, or mitigate, a relevant impact of a physical hazard on a critical site (paragraph (b)); and
- to respond to incidents where unauthorised access to a critical site occurs (paragraph (c)); and
- to control access to critical sites, including restricting access to only those individuals who are critical workers or accompanied visitors (paragraph (d)); and
- 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 (paragraph (e)); and
- to minimise or eliminate a material risk of, or mitigate, a relevant impact of a natural hazard on the asset (paragraph (f)).

The purpose of subsection 11(2) is to ensure that an entity's program contains necessary detail regarding their processes for managing and mitigating a variety of physical and natural hazards to their critical infrastructure assets, as well as recovery procedures for circumstances where a natural hazard disrupts the business operations of the asset.

Subsection 11(3) sets out the matters an entity must have regard to when adopting, reviewing or varying a critical infrastructure risk management program for section 30AKA of the Act.

The matters that the entity must have regard to are:

- whether the asset's critical sites are described in the program (paragraph (d));
- whether the physical hazards, the occurrence of which could have a relevant impact on a critical site, are described in the program (paragraph (e));
- whether the security arrangements for the asset are described in the program (paragraph (f));
- whether the natural hazards, the occurrence of which could have a relevant impact on the asset, are described in the program (paragraph (g)).

Schedule 1 Criminal history criteria

Subsection 9(4) provides requirements for a background check of a critical worker under subsection 9(3). Paragraph 9(4)(b) provides that, if the background check includes a criminal history check, the criteria against which that information must be assessed is the *criminal history criteria* in Schedule 1.

Schedule 1 sets out the criminal history criteria. The offences listed in the Schedule are the criteria against which a criminal history check as part of a background check under the AusCheck scheme will be assessed.

The criminal history criteria are modelled after the MNE-security offences prescribed in Schedule 1 to the *AusCheck Regulations 2017* (AusCheck Regulations) (MNE is acronym for major national event). Separate amendment to the AusCheck Regulations will be required to fully operationalise the conduct of background checks.

Schedule 2 Part 2A critical hospitals

Section 3 defines a *Part 2A critical hospital* as a hospital mentioned in Schedule 2.

Schedule 2 provides a critical hospital is critical hospital located in a State or Territory mentioned in an item of the table that satisfies the description for that item. Accordingly, the effect of this provision is that Part 2A of the Act will only apply to a hospital that meets that description.

The note in the draft instrument states 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 section 4 of the *Security of Critical Infrastructure (Critical infrastructure risk management program) Rules (LIN 22/018) 2022*. Part 2A hospitals are scheduled in the draft instrument by State and Territory in recognition of the variances between jurisdictions for hospitals with general intensive care units (for example, Levels 3 and 4 hospitals may be described against New South Wales). What particular descriptions will be included in the table is subject to further consultation.