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 23/006) 2023

1 The instrument, Departmental reference LIN 23/006, is made under section 61 of the *Security of Critical Infrastructure Act 2018* (the Act).

2 The instrument commences the later of:

- immediately after the *AusCheck Legislation Amendment (Critical Infrastructure Background Check) Regulations 2023* commence; and
- the day after registration.

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

Purpose

3 Part 2A of the 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.

4 A CIRMP is a written program, the purpose of which under paragraph 30AH(1)(b) of the 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.

5 The instrument specifies critical infrastructure assets to which Part 2A of the Act applies and specifies the CIRMP requirements for the responsible entities for those assets. The instrument does this by:

- specifying, for paragraph 30AB(1)(a) of the Act, that Part 2A of the Act applies to the critical infrastructure assets mentioned in the instrument;
- providing, for subsection 30AB(3) of the Act, that Part 2A, including the CIRMP requirements specified in the instrument, apply to a critical infrastructure asset 6 months after the instrument commences or for assets that become CI assets after the instrument commences;

- it is noted responsible entities have a further 12 months from the end of the applicable period to have a process or system in place to comply with a cyber security framework—see subsections 8(3), (4) and (5) of the instrument and relevant explanation below;

- specifying the Reserve Bank of Australia as the ***relevant commonwealth regulator***, for paragraph (a) of that definition in section 5 of the Act, for a critical financial market infrastructure asset mentioned in paragraph 12D(1)(i) of the Act;

- specifying, for paragraph 30AH(1)(c) of the Act, the requirements that a CIRMP must comply with; and

- setting out, for subsections 30AKA (1), (3) and (5) of the Act, matters a responsible entity must have regard to when adopting, reviewing and varying their CIRMP.

Details of the instrument

6 Details of the instrument are set out in **Attachment A**.

Parliamentary scrutiny etc.

7 The instrument is subject to disallowance under section 42 of the Legislation Act. A Statement of Compatibility with Human Rights provides that the 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 reasonable, necessary and proportionate to pursue the legitimate objective of national security and public order. The Statement is included at **Attachment B**.

8 The instrument is made by the Minister for Home Affairs in accordance with the requirements of sections 30ABA, 30AL and 61 of the Act.

9 In particular, before making the instrument, the Minister :

- considered the submissions received during consultation on the instrument (for paragraphs 30ABA(2)(c) and 30AL(2)(c) of the Act);

- had regard to any existing regulatory systems of the Commonwealth, a State or a Territory that imposes obligations on a responsible entity for a critical infrastructure asset (paragraph 30AH(6)(a));

- had regard to the costs that are likely to be incurred by a responsible in complying with the instrument (paragraph 30AH(6)(b));

- had regard to the reasonableness and proportionality of the requirement in the instrument in relation to the purposes referred to in paragraph 30AH(1)(b) (paragraph 30AH(6)(c)).

Consultation

10 The Department of Home Affairs (the Department) engaged industry stakeholders from across critical infrastructure sectors in a consultation process to design the instrument.

11 Before making this instrument, the Minister in accordance with sections 30ABA and 30AL of the Act:

- published a notice on the Department's website:
  - setting out the draft rules made for the purposes of Part 2A of the Act; and
  - inviting 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 45 days, commencing on 5 October 2022 and ending on 18 November 2022); and
- gave a copy of the notice to each State and Territory First Minister; and
- provided notice of the consultation to 2619 stakeholders, inviting written submissions; and
- considered any submissions received, which included 39 written submissions.

12 The following consultation occurred during the period:

- two public virtual Town Halls on 10 October 2022 and 12 October 2022 (257 and 297 attendees, respectively);
- four question and answer sessions on 13 October 2022, 18 October 2022, 25 October 2022 and 1 November 2022 (101, 141, 162 and 101 attendees, respectively);
- ten bilateral meetings at the request of individual stakeholders; and
- twenty email responses to queries.

13 Critical hospitals raised that the definition of *critical hospital* in the Act was too broad for the purposes of Part 2A of the Act. Consultation was undertaken to provide stakeholders with the opportunity to advise which critical hospitals should be subject to Part 2A of the Act. The outcome of this consultation lead to the subset of critical hospitals, 'designated hospitals' being specified in the instrument and to which Part 2A of the Act applies.

14 As part of the consultation process, the Department published a draft Risk Management Program Guidance document on the Department's website. Additionally, the Department created a Frequently Asked Questions document based on queries received throughout the consultation period, which was made publically available on the Department's website.

15 Stakeholder feedback included requests for clarification on the timeframes for compliance, the availability of AusCheck background checks to address personnel security risks, the breadth of consideration required to be given to supply chain hazards and the definition of key terms.

16 In these circumstances, the Minister was satisfied that appropriate consultation was undertaken, in accordance with section 17 of the Legislation Act because:

- persons likely to be affected by the instrument had an adequate opportunity to comment on the draft instrument; and
- the draft instrument was initially developed and subsequently refined by drawing upon the knowledge and expertise of stakeholders; including:
    - owners and operators of assets, and
    - the Reserve Bank of Australia to the extent that assets relate to critical financial market infrastructure assets.

17 A regulation impact statement (RIS) was conducted in relation to the measures in the instrument (OBPR-02914) (**Attachment C**). The RIS is informed by extensive consultation with stakeholders and identifies the regulatory impact of the reforms. The RIS weighs the regulatory costs of the measures 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 the instrument, is minimal when compared to the damage to the economy if businesses underinvest in security and allow breaches to occur.

18 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.

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

Attachment A

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

Section 1 Name

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

Section 2 Commencement

This section provides that the instrument commences on the later of:

- immediately after the *AusCheck Legislation Amendment (Critical Infrastructure Background Check) Regulations 2023* (the amendment regulations) commence; and
- the day after registration.

This ensures the instrument will not commence until after the amendment regulations commence. If the amendment regulations never commence, the instrument will never commence. This is because certain provisions in the instrument are dependent on the amendment regulations.

Section 3 Definitions

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

For example, the instrument provides that ***personnel hazard*** includes where a person acts, through malice or negligence, to compromise the proper function of the asset or cause significant damage to the asset. The instrument also provides definitions for ***cyber and information security hazard***, ***natural hazard***, ***physical security hazards*** and ***supply chain hazard***. The matters included in those definitions are not intended to be exhaustive. The responsible entity must determine what matters expressed in these definitions are relevant to the operation of the entity's critical infrastructure asset(s).

Section 4 Application of Part 2A of the Act

Subsection 4(1) of the instrument specifies, for paragraph 30AB(1)(a) of the *Security of Critical Infrastructure Act 2018* (the Act), that Part 2A of the Act applies to a critical infrastructure asset mentioned in paragraphs 4(1)(a) to (m) of the instrument.

Paragraph 4(1)(g) of the instrument specifies a ***designated hospital***. A designated hospital is a hospital that is a critical hospital (see the definition of that term in section 5 of the Act) mentioned in Schedule 1 to the instrument—see also section 3 and Schedule 1 to the instrument. This represents a subset of critical hospitals that are considered appropriate to apply Part 2A of the Act to. See further detail about consultation above.

Delayed application of Part 2A

Subsection 4(2) of the instrument provides, for subsection 30AB(3) of the Act, that Part 2A of the Act (including the requirements in the instrument) will apply to a critical infrastructure asset mentioned in subsection 4(1) of the instrument on the later of:

- 6 months after the instrument commences; and
- 6 months after the asset became a critical infrastructure asset.

For assets that are a critical infrastructure asset on the day the instrument commences, Part 2A applies 6 months after the instrument commences. If an asset becomes a critical infrastructure asset after the instrument commences, Part 2A will apply to the asset 6 months from that date. For example, if an asset becomes a critical infrastructure asset on 1 March 2023, Part 2A (including the instrument) will apply to the asset on 1 September 2023.

The purpose of subsection 4(2) of the instrument is to provide responsible entities with a reasonable timeframe to establish and begin complying with their CIRMP before Part 2A of the Act applies to their critical infrastructure asset.

In addition to the initial 6 month period where Part 2A of the Act does not apply to a critical infrastructure asset, subsection 8(3) of the instrument provides a further 12 month period to comply with the cyber and information security requirements specified in subsection 8(4) or 8(5) of the instrument.

See section 8 for further details.

Application of instrument to critical infrastructure assets specified in other instruments

Subsection 4(3) of the instrument provides that requirements specified in the instrument for paragraph 30AH(1)(c) and sections in the instrument made for subsections 30AKA(1), (3) and (5) of the Act apply to an asset:

- that is specified in subsection 4(1) of the instrument, and that is not specified in any other rules made for paragraph 30AB(1)(a) of the Act; or
- referred to in paragraph 30AB(1)(b) of the Act.

This clarifies that the requirements in the instrument only apply to a critical infrastructure asset that is specified in the instrument for paragraph 30AB(1)(a) of the Act, or an asset privately declared under section 51 to be a critical infrastructure asset including a determination that Part 2A applies to the asset. This ensures that critical infrastructure assets specified in other rules made for paragraph 30AB(1)(a) of the Act will not be required to comply with the requirements of the instrument. For example, the *Security of Critical Infrastructure (Naval Shipbuilding Precinct) Rule (LIN 22/007) 2023* is intended to be made at the same time as the instrument and specifies requirements unique to the critical infrastructure assets specified in that instrument.

Section 5 Relevant Commonwealth regulator

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

This provides that, in accordance with paragraph 30AG(2)(b) of the Act for example, responsible entities will be required to give their annual report to the RBA.

Part 2 Requirements for a critical infrastructure risk management program

Section 6 Material risk

Section 6 of the instrument sets out that, under subsection 30AH(8) of the Act, material risk includes:

- a stoppage or major slowdown of the asset's functioning for an unmanageable period (paragraph (a));
- a substantive loss of access to, or deliberate or accidental manipulation of, a critical component of the critical infrastructure asset (paragraph (b));
- an interference with the critical infrastructure asset's operating technology or information communication technology essential to the functioning of the asset (paragraph (c));
- the storage, transmission or processing of *sensitive operational information* outside Australia (paragraph (d));
- remote access to operational control or operational monitoring systems of the critical infrastructure asset (paragraph (e)).

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

- identify hazards where there is a material risk (i.e. one of the risks outlined above) that could have a relevant impact on the asset if it occurred (subparagraph 30AH(1)(b)(i) of the Act); and
- establish and maintain a process or system in a CIRMP to—as far as it is reasonably practicable to do so—minimise or eliminate the material risks of such a hazard occurring (subparagraph 30AH(1)(b)(ii) of the Act).

Responsible entities must do this in relation to all hazards—including those specified in the instrument (e.g. personnel hazards) and any other hazard identified by the responsible entity. The purpose of section 6 is to specify certain 'material risks' for subsection 30AH(8) of the Act that a CIRMP must address with respect to those hazards.

For example, paragraph 6(d) of the instrument specifies that *'the storage, transmission or processing of sensitive operational information outside Australia'* is a material risk. Sensitive operational information includes, among other things, layout diagrams, schematics and geospatial information. The failure for a CIRMP to minimise or eliminate material risks may lead to the occurrence of hazards that have a relevant impact on a critical infrastructure asset (as defined in section 8G of the Act).

Section 7 General—all hazards

Subsection 7(1) of the instrument specifies, for paragraph 30AH(1)(c) of the Act, that in relation to all hazards, responsible entities must establish and maintain a process of system in their CIRMP:

- to identify the operational context of each CI asset (paragraph (a)); and
- to identify the material risks to the asset (paragraph (b)); and
- as far as it is reasonably practicable to do so:
    - to minimise or eliminate the material risks, which may include those mentioned in section 6 (subparagraph (c)(i)); and
    - to mitigate the relevant impact of each hazard on the asset (subparagraph (c)(ii)); and
- to review the CIRMP to ensure compliance with section 30AE of the Act (paragraph (d)); and
- to keep the CIRMP current to ensure it complies with section 30AF of the Act (paragraph (d)).

This specifies what a CIRMP must do generally to address all hazards, including hazards not identified in the instrument. These requirements provide a responsible entity with specific measures that the CIRMP needs to implement.

Subsection 7(2) of the instrument sets out, for subsections 30AKA(1), (3) and (5) of the Act, matters a responsible entity must have regard to in deciding to adopt, review or vary a CIRMP. These are whether the program:

- describes the outcome of the process or system mentioned in paragraph (1)(a) (paragraph (a));
- describes interdependencies between each of the entity's critical infrastructure assets and other critical infrastructure assets (paragraph (b));
- identifies each position within the entity (paragraph (c)):
    - that is responsible for developing and implementing the CIRMP (subparagraph (c)(i)); and
    - for the processes mentioned in paragraph (1)(d)—that is responsible for reviewing the program or keeping the program up to date (subparagraph (c)(ii));
- contains the contact details for the positions described under paragraph (c) (paragraph (d));
- contains a risk management methodology (paragraph (e));
- describes the circumstances in which the entity will review the program (paragraph (f)).

This may include matters such as how the CIRMP will function on a daily basis, the kinds of relevant impacts that are most applicable to the assets, interaction with other critical infrastructure assets across and within sectors, an overview of the process of risk management methodology that the CIRMP uses.

Section 8 Cyber and information security

Section 8 of the instrument sets out the requirements that an entity's CIRMP must comply with for cyber and information security hazards.

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

Subsection 8(2) of the instrument provides that the entity must establish and maintain a process or system in the CIRMP to—as far as it is reasonably practicable to do so:

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

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

The purpose of subsection 8(2) is to require an entity's program to have a sufficient level of preparedness to reduce to likelihood of a cyber and information security hazard having a relevant impact on the asset (see section 8G of the Act).

Subsection 8(3) of the instrument provides that, within 12 months after the end of the applicable 6 month period mentioned in subsection 4(2) of the instrument, a responsible entity must comply with *either* subsection 8(4) or 8(5) of the instrument, which respectively require a responsible entity to establish and maintain a process or system in their CIRMP to comply with a specified cybersecurity framework or an equivalent framework.

The purpose of subsection 8(3) is to provide a responsible entity with additional time to build up the cyber and information security capability of their critical infrastructure asset as part of their CIRMP. Accordingly, an entity will have a total of 18 months to comply with *either* subsection 8(4) or 8(5) of the instrument.

For example, if the instrument commenced on 1 January 2023, then an asset that is a critical infrastructure asset on this date will have Part 2A apply to it from 1 July 2023. The responsible entity will then have a further 12 months to comply with the requirements in *either* subsection 8(4) or 8(5) of the instrument—being 1 July 2024. If an asset becomes a critical infrastructure asset on 1 March 2023 (i.e. became a CI asset after the instrument commenced), the responsible entity will be required to comply with this provision for a total of 18 months after that date—1 September 2024.

Paragraph 8(4)(a) of the instrument requires a responsible entity to establish and maintain a process or system in the CIRMP to comply with a framework contained in a document mentioned in the table, as in force from time to time. Paragraph 8(4)(b) of the instrument requires that if there is a condition mentioned for the document, the entity must also meet the condition. The documents listed in the table are:

- Australian Standard *AS ISO/IEC 27001:2015* (item 1)—which is the Australian Standard that directly adopts the requirements of International Standard ISO 27001;

- *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 condition that the entity is required to meet Security Profile 1 (item 5).

The purpose of subsection 8(4) is to require a responsible entity's CIRMP to meet a baseline level of cyber and information security for their critical infrastructure asset. The requirement to comply with or meet does not prohibit a responsible entity from exceeding the requirements – the instrument establishes a baseline standard in this regard.

In the event that a framework mentioned in subsection 8(4) of the instrument is updated or changes, an entity is required to meet the updated requirements as soon as reasonably practicable (see sections 30AE and 30AF of the Act).

The note to subsection 8(4) provides that sections 30AN and 30ANA of the Act enable the incorporation of some of the documents mentioned in this subsection as in force from time to time.

The purpose of this note is to provide that, despite subsection 14(2) of the Legislation Act, rules made for sections 30AH or 30AKA of the Act may make provision in relation to a matter by applying, adopting or incorporating, with or without modification any matter:

- contained in a standard proposed or approved by Standards Australia as in force or existing from time to time;

- contained in a *relevant document* (see subsection 30ANA(2) of the Act) as in force or existing from time to time.

Sections 30AN and 30ANA of the Act enable the incorporation by reference of the documents mentioned in subsection 8(4), as in force from time to time. This is for best practice guidelines and processes to be adopted as part of a CIRMP.

Subsection 8(5) of the instrument requires a responsible entity to establish and maintain a process or system in the CIRMP to comply with a framework that is equivalent to a framework contained in a document mentioned in subsection 8(4) of the instrument (including any conditions mentioned for the framework).

The purpose subsection 8(5) is to provide responsible entities with the flexibility to comply with their statutory obligations by recognising alternative cyber security frameworks that achieve the desired uplift in security and resilience of the Part 2A asset. As stated above, a responsible entity must comply with subsection 8(4) or 8(5) of the instrument.

Subsection 8(6) of the instrument provides that, for subsections 30AKA(1), (3) and (5) of the Act, a responsible entity must have regard to whether the CIRMP describes the cyber and information security hazards that could have a relevant impact on the critical infrastructure asset.

Section 9 Personnel hazards

Section 9 of the instrument sets out requirements that a CIRMP must comply with for personnel hazard.

Subsection 9(1) of the instrument provides that, for personnel hazards, for paragraph 30AH(1)(c) of the Act, a responsible entity must establish and maintain a process or system in the entity's CIRMP:

- to identify the entity's critical workers (paragraph (1)(a));
- 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; (paragraph (1)(b)); and
- as far as it is reasonably practicable to do so—to minimise or eliminate material risks (paragraph (1)(c)):
    - arising from malicious or negligent employees or contractors (subparagraph (c)(i));
    - arising from the off-boarding process for outgoing employees and contractors (subparagraph (c)(ii));

Subsection 9(2) of the instrument, for paragraph 30AH(4)(a) of the Act, provides that the process and 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

The note to the provision clarifies that a responsible entity is not required to use the AusCheck scheme to assess the suitability of critical workers, however, they may choose to do so. Responsible entities may use other schemes to assess the suitability of critical workers. Alternative schemes should be detailed in a CIRMP.

In making a suitability assessment for paragraph 9(1)(b), a responsible entity must consider the matters set out in subsection 9(5) of the instrument.

Requirements for a background check if conducted under the AusCheck scheme

Subsection 9(3) of the instrument provides that, if a CIRMP permits a background check to be conducted under the AusCheck scheme, 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*—respectively an individual's criminal history, a security assessment of an individual under the ASIO Act, an individual's immigration status, and the identity of the individual.

The background check must:

- for paragraph 30AH(4)(c) of the Act—assess information relating to the individual's criminal history against the criminal history criteria (paragraph (a)); and
- for paragraph 30AH(4)(d) of the Act—an assessment of information relating to the identity of the individual must consist of an electronic identity verification check and in person identity verification check (paragraph (b)).

Subsection 9(4) of the instrument provides that a responsible entity must notify the Secretary of the Department if a background check is no longer required for a person. The purpose of this subsection is to ensure that a responsible entity is actively managing and updating the status their background checks, including those of outgoing employees and contractors.

The overarching purpose of section 9 of the instrument is to ensure that responsible entities obtain relevant information through a suitability assessment process. This will empower them to consider whether a person is

suitable to be permitted access to the critical infrastructure asset, or determine a suitable mitigation strategy where necessary.

Requirements for a suitability assessment of a critical worker for a CIRMP

Subsection 9(5) of the instrument provides that, in making a suitability assessment for paragraph 9(1)(b) of the instrument, a responsible entity must consider the following:

- any advice from the Secretary of the Department under the following provisions of the *AusCheck Regulations 2017* (AusCheck Regulations):
    - paragraph 21DA(2)(a)—whether or not the individual has an unfavourable criminal history (subparagraph (a)(i));
    - paragraph 21DA(2)(b)—whether or not the security assessment of the individual is an adverse security assessment or qualified security assessment (subparagraph (a)(ii));
    - subsection 21DA(4)—whether there has been a material change in the individual's criminal history if the individual had an unfavourable criminal history from the last background check (subparagraph (a)(iii));
    - subsection 21DA(5)—details of the relevant CIRMP offence and any sentence imposed for the offence where the individual expressly consents for those details to be provided to the responsible entity (subparagraph (a)(iv)); and
- whether permitting a critical worker to have access to critical components of the CI asset would be prejudicial to security (paragraph (b)); and
- any other information that may impact the person's suitability to have unescorted access to the asset (paragraph (c)).

Responsible entities must consider these matters, regardless of whether a background check under the AusCheck scheme was utilised. The phrase 'any advice' in paragraph 9(5)(a) acknowledges that such advice from the Secretary will not be provided in all cases. However, where it is, it must be considered by the responsible entity, as well as the matters mentioned in paragraphs 9(5)(b) and (c) of the instrument, when making a suitability assessment.

This subsection requires responsible entities to consider the security risk of an individual. Where the AusCheck scheme is utilised, in particular, a background check will provide relevant information to enable them to take steps to control or limit access to the critical infrastructure asset, as required.

The note contained at subsection 9(5) of the instrument reminds responsible entities of the obligation, under section 21ZA of the AusCheck Regulations, to inform the Secretary of certain decisions the responsible entity takes.

Subsection 9(6) of the instrument provides that, for subsections 30AKA(1), (3) and (5) of the Act, a responsible entity must have regard to the following matters:

- whether the CIRMP lists the entity's critical workers (paragraph (a));

- whether the CIRMP describes the personnel risks which could have a relevant impact on the asset (paragraph (b)).

Section 10 Supply chain

Section 10 of the instrument specifies, for paragraph 30AH(1)(c) of the Act, the processes or systems that a CIRMP must have for supply chain hazards.

Paragraph 10(1)(a) of the instrument, provides that a responsible entity must establish and maintain in its CIRMP a process or system to, as far as it is reasonably practicable—minimise or eliminate the material risk of:

- unauthorised access, interference or exploitation of the asset's supply chain (subparagraph (i));
- misuse of privileged access to the asset by any provider in the supply chain (subparagraph (ii));
- disruption of the asset due to an issue in the supply chain (subparagraph (iii));
- threats to people, assets, equipment, products, services, distribution and intellectual property within supply chains (subparagraph (iv));
- major suppliers (subparagraph (v)) and
- any failure or lowered capacity of other assets and entities in the entity's supply chain (subparagraph (vi)).

Paragraph 10(1)(b) of the instrument, provides that a responsible entity must establish and maintain in its CIRMP a process or system to, as far as it is reasonably practicable— mitigate the relevant impact of a supply chain hazard on the asset.

These requirements are intended to ensure that a CIRMP addresses vulnerabilities in an entities' supply chain in areas such as security, suppliers and logistics.

Subsection 10(2) of the instrument provides that, for subsections 30AKA(1), (3) and (5) of the Act, a responsible entity must have regard to the following matters:

- whether the CIRMP lists the entity's major suppliers (paragraph (a)); and
- whether the supply chain hazards, which could have a relevant impact on the asset, are described in the CIRMP (paragraph (b)).

Under this provision, an entity should consider whether their CIRMP adequately identifies hazards throughout the supply chain that could impact the availability, integrity, reliability or confidentiality of the critical infrastructure asset if they were to occur.

Section 11 Physical security hazards and natural hazards

Section 11 of the instrument specifies, for paragraph 30AH(1)(c) of the Act, the processes or systems that a CIRMP must have for physical security hazards and natural hazards.

Subsection 11(1) of the instrument provides that, for physical security hazards and natural hazards, a responsible entity must establish and maintain a process or system in the entity's CIRMP:

- to identify the physical critical components of the critical infrastructure asset (paragraph (a)); and
- as far as it is reasonably practicable—to minimise or eliminate the material risk of:
    - a physical security hazard on a physical critical component (subparagraph (b)(i)); and
    - a natural hazard on the asset (subparagraph (b)(ii)); and
- to respond to incidents where unauthorised access to a physical critical component occurs (paragraph (c)); and
- to control access to physical critical components, 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)).

The purpose of subsection 11(1) is to require entities to develop processes or systems in their CIRMP for managing and mitigating a variety of physical security hazards and natural hazards to their critical infrastructure assets.

A 'physical critical component' as mentioned in section 11 specifically refers only to those tangible or material parts of an asset where the absence of, damage to or compromise of the part would prevent the proper function of the asset or could cause significant damage to the asset (e.g. gas transmission pipeline control room). This is in contrast to *critical component* (as defined in section 3 of the Act), which also encompass intangible assets, such as software and computer data, which would not be considered physical critical components for the purpose of section 11 of the instrument.

Subsection 11(2) of the instrument provides that, for subsections 30AKA(1), (3) and (5) of the Act, a responsible entity must have regard to whether:

- the asset's physical critical components are described in the CIRMP (paragraph (a));
- the physical hazards, the occurrence of which could have a relevant impact on a physical critical component, are described in the CIRMP (paragraph (b));
- the security arrangements for the asset are described in the CIRMP (paragraph (c));
- the natural hazards, the occurrence of which could have a relevant impact on the asset, are described in the CIRMP (paragraph (d)).

Under this provision, a responsible entity should consider whether their CIRMP adequately identifies and details the physical security hazards and natural hazards that could impact the availability, integrity, reliability or confidentiality of their physical critical components.

Schedule 1 Designated hospital

Schedule 1 sets out the list of critical hospitals to which Part 2A of the Act applies. Designated critical hospital is defined in section 3 of the instrument, and is explained above.

Consultation in relation to these hospitals is also explained above.

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

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

1 The *Security Legislation Amendment (Critical Infrastructure Protection) Act 2022* (SLACIP Act) amended the *Security of Critical Infrastructure Act 2018* (SOCI Act) to include Part 2A, requiring certain responsible entities for critical infrastructure assets to adopt, maintain and comply with an all-hazards critical infrastructure risk management program.

2 The *Security of Critical Infrastructure (critical infrastructure risk management program) Rules (LIN 23/006) 2023* 'switch on' the Part 2A obligations and specify what the responsible entity must establish and maintain in the entity's program.

3 The purpose of the instrument is to enhance Government and industry's understanding of the threat environment facing Australia's critical infrastructure and building the security and resilience of critical infrastructure assets against national security incidents impacting businesses and the Australian economy.

- The instrument require responsible entities to:
    - Identify all-hazards where there is a material risk of that hazard causing a relevant impact on the asset; and to minimise or eliminate those material risks to the extent reasonably practicable; and to mitigate the relevant impact of such a hazard on the asset to the extent reasonably practicable.
- A responsible entity must provide an annual report to the relevant Commonwealth regulator relating to its critical infrastructure risk management program under subsection 30AG(2) of the SOCI Act. If the entity has a board, council or other governing body, the annual report must be approved by the board, council or other governing body.

4 The instrument specify that Part 2A applies to the following critical infrastructure assets:

- Communication sector: critical broadcasting assets, and critical domain name system;
- Data storage or processing sector: critical data storage or processing assets;
- Financial services and markets sector: critical payment systems assets;

- Health care and medical sector: critical hospital;
- Transport sector: critical freight infrastructure assets and critical freight services assets;
- Water and sewerage sector: critical water assets;
- Food and grocery sector: critical food and grocery assets;
- Energy sector: critical electricity assets, critical gas assets, critical liquid fuel assets and critical energy market operator assets.

5 Responsible entities of these critical infrastructure assets are required to comply with the instrument.

6 The instrument is principles-based requiring responsible entities to consider the material risk/s to their critical asset/s – covering the following domains:

- physical security hazards and natural hazards;
- cyber and information security hazards;
- personnel security hazards; and
- supply chain hazards.

7 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 instrument and inviting persons to make submissions to the Minister about the draft instrument or amendments during a consultation period no shorter than 28 days. The Minister opened consultation on the draft instrument for a period of 45 days, from 5 October 2022 to 18 November 2022. The Minister gave a copy of the notice to each First Minister. The Minister considered all submissions received within the consultation period.

8 The instrument seek to minimise the security and economic impact on industry from its ongoing exposure to the risks associated with all hazards. Emerging risks are rapidly outpacing the current regulatory environment.

9 The cost to Australia's critical infrastructure assets extends beyond the responsible entities themselves in the event of a serious incident. For example, an incident in the energy sector has the ability to inhibit critical infrastructure assets such as hospitals, water assets and transport assets.

10 One event could have a catastrophic impact on the ability for critical infrastructure to service Australia, which would in turn have cascading failures across society and the entire Australian economy.

11 By raising security for critical infrastructure assets, the instrument broadly supports the human rights of persons in Australia by, among other things, supporting an adequate standard of living, high standards of health and access to medical services.

Human rights implications

This instrument engages the following rights:

- The right to an adequate standard of living, including food in Article 11 of the *International Covenant on Economic, Social and Cultural Rights* (ICESCR)
  The right to the highest attainable standard of physical and mental health including medical service and medical attention in Article 12 of the ICESCR
- The right to privacy in Article 17 of the *International Covenant on Civil and Political Rights* (ICCPR)

The right to an adequate standard of living, including food

1. Article 11 of the ICESCR provides for the right of everyone to an adequate standard of living, including adequate food, clothing and housing and the continuous improvement of living conditions. Article 11 commits States Parties to the Covenant to take measures to safeguard these standards.

2. This instrument requires responsible entities of critical infrastructure assets to manage risks that hazards may pose to the continued operation of critical infrastructure assets which may impact the supply of products and services essential to an adequate standard of living.

3. For example, the instrument may require the responsible entities for critical food and grocery assets to manage supply chain risks. This would reduce the likelihood of a disruption to the food and grocery supply chain which could impact the production, distribution and availability of food. The instrument may also require the responsible entities for critical water or energy sector assets to manage risks, to ensure that risks to adequate energy and clean water supplies are mitigated or that risks to the finance sector are mitigated so that a person's ability to pay for essential services or obtain adequate food and clothing is not disrupted.

4. A comprehensive set of rules to manage risks enhances an adequate standard of living by recognising the role that critical infrastructure assets may play in delivering essential supplies that maintain and sustain life.

5. Overall, requiring responsible entities to comply with Rules will reduce the likelihood of a disruption to distribution networks and other key operations of Australia's major critical infrastructure assets, which could impact the availability of products and services that support an adequate standard of living, promoting the right to an adequate standard of living.

The right to the highest attainable standard of physical and mental health including medical service and medical attention

6. Article 12 of the ICESCR provides for the right of everyone to the enjoyment of the highest attainable standard of physical and mental health, including medical service and medical attention in the event of sickness. The United Nations Committee on Economic, Social and Cultural Rights has stated that the right to health embraces a wide range of socio-economic factors that promote conditions in which people can lead a healthy life, and extends to the underlying determinants of health.

7. This instrument requires responsible entities of critical infrastructure assets to manage risks that hazards may pose to the continued operation of critical infrastructure assets that may impact the supply of products and services essential to obtaining the highest attainable standard of physical and mental health.

8. Hospitals are crucial to Australia's ability to fulfil this obligation as they provide critical care for patients with a variety of medical, surgical and trauma conditions, and are therefore integral to the sustainment of life.

9. This instrument takes into consideration critical infrastructure assets with a high degree of interdependency with critical hospitals, will assist to protect these important assets, and in turn, the physical and mental health of all persons in Australia.

10. For example, an attack on a critical hospital could pose a risk to life. Similarly, the consequences of a prolonged and widespread failure in the energy sector could cause shortages or destruction of essential medical supplies. Improving business resilience and protecting the asset should it be subject to a significant cyber attack will reduce the likelihood of a disruption to the provision of essential medical services and ensure appropriate services remain available in the event of sickness, promoting the right to the right to the highest attainable standard of physical and mental health.

The right to privacy

11. Article 17(1) of the ICCPR provides that no one shall be subjected to arbitrary or unlawful interference with their privacy.

12. Section 7(2)(f), section 7(2)(g) and section 9(2)(a) of this instrument engage the right to privacy by requiring that responsible entities identify contact details of its critical positions and critical personnel in their risk management program. Critical personnel, by example, may be an employee of the responsible entity. This requires responsible entities to collect and store personal information, including the names of certain employees.

13. Although the collection of personal information limits the right to privacy, the limitation is reasonable, necessary and proportionate in achieving the legitimate objective of protecting national security and public order. Requiring responsible entities to identify the contact details for critical positions and critical personnel in their risk management program helps to ensure that risks to critical infrastructure that may be posed by certain hazards, such as personnel, can be mitigated, as the most critical personnel may need to be quickly identified including immediately prior, during or following a significant cyber security incident to manage the risk. Critical personnel have responsibility, access, control or management of the essential components or systems of critical infrastructure assets. The fact that the absence or compromise of critical personnel may have a cascading impact on the proper functioning of the asset also demonstrates the role critical personnel may have in restoring the proper functioning of the asset during a cyber incident.

14. Requiring responsible entities to identify contact details is necessary to pursue the objective of national security. This may also be necessary to pursue other objectives such as public order including protecting health where the Rules made by the Minister may apply to designated hospitals. Collecting information of employees of responsible entities helps protect critical infrastructure from employees who could be ‘trusted insiders’ who lead to disruption in the provision of essential services. Trusted insiders are potential, current or former employees or contractors who have legitimate access to information, techniques, technology, assets or premises. Trusted insiders can intentionally or unknowingly assist external parties in conducting activities against the organisation or can commit malicious acts of self-interest. Such action by a trusted insider can undermine or severely impact the availability, integrity, reliability or confidentiality of those assets captured as critical infrastructure assets. Maintaining personal details and individualised access allows an entity to quickly revoke or amend access to critical systems and physical components if a potential malicious insider is identified. Where such an event poses a risk to national security personal details may be shared with law enforcement agencies to assist them in responding to the event.

15. Appropriate safeguards exist to ensure that any use of an individual’s personal information is reasonable and proportionate. The responsible entity is only required to include contact details for the personnel who are deemed critical. Restricting the collection of contact details to critical personnel safeguards against the arbitrary collection of personal information of all personnel. Furthermore it is reasonable to believe that the responsible entity would already hold this personal information from critical personnel who have consented to work for the responsible entity.

16. The instrument also enable a responsible entity to conduct a background check on critical employees through AusCheck. To the extent that the responsible entity submits a critical employee's personal information for an AusCheck background check, the right to privacy will be engaged. However, it is reasonable, necessary and proportionate to limit the right to privacy in this way. Background checks on critical employees may be necessary where a responsible entity is assessing the suitability of a critical worker to have access to the critical components of the asset. This enables the responsible entity to ensure that only persons suitable to the role are engaged as critical employees.

17. Personal information is provided voluntarily by an individual with their express consent to it being used for a background check. An individual will be provided with a privacy notice by AusCheck detailing how their information will be used to ensure consent is fully informed.

18. The collection, use and disclosure of personal information for the purposes of an AusCheck background check is authorised by the *AusCheck Act 2007* and the *AusCheck Regulations 2017* (AusCheck Regulations). The *AusCheck Legislation (Critical Infrastructure Background Check) Regulations 2023* will amend the AusCheck Regulations to include critical infrastructure background checking within the AusCheck scheme. This instrument requires responsible entities to establish and maintain a process to assess the suitability of a critical worker to have access to critical components of a critical infrastructure asset. The instrument enables the responsible entity to conduct an AusCheck background check for that purpose. To the extent that instrument enables a responsible entity to disclose information to AusCheck, use of this information is reasonable and necessary to pursue the objective of mitigating against personnel hazards to critical infrastructure assets and the essential services delivered by them.

Conclusion

The 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 reasonable, necessary and proportionate to pursue the legitimate objective of national security and public order.

The Honourable Clare O'Neil MP
Minister for Home Affairs