EXPLANATORY STATEMENT

Issued by authority of the Minister for Home Affairs

Security of Critical Infrastructure Act 2018

Security of Critical Infrastructure (Naval shipbuilding precinct) Rules (LIN 23/007) 2023

1 The instrument is made under section 61 of the *Security of Critical Infrastructure Act 2018* (the Act).

2 The instrument commences on the later of:

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

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

Purpose

3 Part 2A of the Act provides that a 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 prescribes the naval shipbuilding and sustainment assets at the Osborne Naval Shipyard on the Lefevre Peninsula, South Australia as critical infrastructure assets. This has the effect of extending the Part 2A obligations to those critical infrastructure assets and relevant responsible entities. The instrument does this by:

- prescribing, for paragraph 9(1)(f) of the Act, that an asset within a naval shipbuilding precinct that is owned or operated by an entity for the purpose of naval shipbuilding and sustainment as a critical infrastructure asset (see further detail in Attachment A);
- prescribing, for subsection 12L(23) of the Act, the responsible entity for the prescribed critical infrastructure asset;
- specifying, for paragraph 30AH(1)(a) of the Act, that Part 2A of the Act applies to the critical infrastructure assets;

- providing, for subsection 30AH(3) of the Act, that Part 2A, including the CIRMP requirements specified in the instrument, apply to the critical infrastructure assets 12 months after the instrument commences;

- specifying the Department of Defence as the ***relevant commonwealth regulator***, for paragraph (a) of that definition in section 5 of the Act, for the critical infrastructure assets; and

- specifying, for paragraph 30AH(1)(c), the requirements that a CIRMP must comply with.

Consultation

6 The Department of Home Affairs (the Department) engaged industry stakeholders from across the naval shipbuilding sector in a consultation process to design the instrument.

7 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 34 days, commencing on 5 August 2022 and ending on 7 September 2022); and
- gave a copy of the notice to each State and Territory First Minister; and
- considered any submissions received, which included 8 submissions.

8 Following the end of the consultation period the Department undertook additional consultation with industry stakeholders from across the naval shipbuilding sector to address submissions and refine the draft instrument. This included:

- Town Hall meetings on 4 August 2022 and 22 August 2022, which were co-hosted by the Department and the Department of Defence, for all identified industry stakeholders at Osborne Naval Shipyard;
- targeted meetings at Osborne Naval Shipyard on 24 August 2022, where impacted industry stakeholders were invited to meet directly with representatives of the Department and the Department of Defence;
- further targeted industry meetings at Osborne Naval Shipyard, on 20 October 2022, where organisations that made submissions during the formal consultation period were invited to discuss their submissions further with representatives from the Department and the Department of Defence.

9 Stakeholder feedback included requests for clarification regarding how the obligations would be applied by Australian Naval Infrastructure Pty Ltd (ABN 45 051 762 639) as the responsible entity in circumstances where the Osborne Naval Shipyard is a multi-user facility or hub with tenants that include government business enterprises and private businesses. To address this concern, a map of the Osborne Naval Shipyard has been incorporated into the Schedule 1 of the instrument to better identify which entity owns or operates assets within the shipyard. This provides certainty as to which entity must comply with obligations under Part 2A of the Act as the responsible entity.

10 In these circumstances, the Minister is 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 within the naval shipbuilding sector, including:
    - owners and operators of assets used for the purposes of naval shipbuilding and sustainment within the Osborne Naval Shipyard, and
    - the Department of Defence to the extent that the assets relate to the defence industry sector.

11 The Office of Best Practice Regulation (OBPR) was consulted and considered that the instrument dealt with matters of a minor nature and no regulatory impact statement was required. The OBPR reference number is 44773.

Details of the instrument

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

Parliamentary scrutiny etc.

13 The instrument is subject to disallowance under section 42 of the Legislation Act. A Statement of Compatibility with Human Rights has been prepared in relation to the instrument, and provides that to the extent that the instrument impacts human rights, the impact is reasonable and proportional. The Statement is included at **Attachment B**.

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

15 In particular, before making the instrument, in accordance with subsection 30AH(6) of the Act, the Minister had regard to the following matters:

- any existing regulatory systems of the Commonwealth, a State or a Territory that imposes obligations on a responsible entity for an asset within a naval shipbuilding precinct (paragraph 30AH(6)(a));
- the costs that are likely to be incurred by a responsible entity for an asset within a naval shipbuilding precinct in complying with the rules (paragraph 30AH(6)(b));
- the reasonableness and proportionality of the requirement in the rules in relation to the purposes referred to in paragraph 30AH(1)(b) (paragraph 30AH(6)(c)).

Attachment A

Details of the *Security of Critical Infrastructure (Naval shipbuilding precinct) Rules (LIN 23/007) 2023*

Part 1 Preliminary

Section 1 Name

This section provides that the name of the instrument is the *Security of Critical Infrastructure (Naval shipbuilding precinct) Rules (LIN 23/007) 2023*.

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 matters included in that definition are not intended to be exhaustive. The responsible entity must determine what matters expressed in these definitions are relevant to the operation of a critical infrastructure asset.

Section 4 Critical infrastructure asset

Subsection 4(1) of the instrument prescribes, for paragraph 9(1)(f) of the Act, that an asset is a critical infrastructure asset if it is within an area identified, using a colour, on the map in Schedule 1 and it is owned or operated for naval shipbuilding or sustainment.

The map in Schedule 1 is a map of Osborne Naval Shipyard. The identified areas are areas of the shipyard used for shipbuilding or sustainment purposes. Areas which have not been identified include carparks, and other areas for which it is unnecessary to apply Part 2A of the Act.

In accordance with the requirement in subsection 9(3) of the Act, before making the instrument the Minister was satisfied:

- that the assets are critical to the defence of Australia or national security (paragraph 9(3)(a) of the Act); and
- that the assets relate to a ***critical infrastructure sector*** (paragraph 9(3)(b) of the Act). Critical infrastructure sector includes the ***defence industry sector*** (see paragraph 8D(k) of the Act); and
- that the assets relate to the defence industry sector.

Subsection 4(2) of the instrument prescribes, for subsection 12L(23) of the Act, the responsible entity for a critical infrastructure asset mentioned in subsection 4(1) is the entity mentioned in Schedule 1 of the instrument for the identified area, which may itself be a critical infrastructure asset, or the location of a critical infrastructure asset.

Osborne Naval Shipyard is a multi-user hub, with multiple entities operating there for the purposes of naval shipbuilding and sustainment. There are four responsible entities for the identified areas at Osborne Naval Shipyard. This reflects the operating nature of Osborne Naval Shipyard, ensures that the most appropriate entity is the responsible entity for each critical infrastructure asset, and that the CIRMP is adopted and complied with, as necessary and appropriate.

Section 5 Application of Part 2A of the Act

Subsection 5(1) of the instrument specifies, for paragraph 30AB(1)(a) of the Act, that Part 2A of the Act applies to a critical infrastructure asset as identified in the map of Osborne Naval Shipyard contained in Schedule 1 of the instrument.

Subsection 5(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 12 months after it becomes a critical infrastructure asset.

For assets that will become a critical infrastructure asset on the day the instrument commences, Part 2A applies 12 months after the instrument commences. If an asset becomes a critical infrastructure asset after the instrument commences, Part 2A will apply to the asset 12 month from that date. It is noted that if additional areas of Osborne Naval Shipyard are to be captured, an instrument amendment would be required. An asset may only become a critical infrastructure asset after the instrument commences if it is, or is within, an area identified by a colour on the map in Schedule 1 and is owned or operated for shipbuilding and sustainment purposes. 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 March 2024.

The purpose of subsection 5(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.

Subsection 5(3) of the instrument provides that the requirements in the instrument, for paragraph 30AH(1)(c) of the Act, apply to a critical infrastructure asset if it is mentioned in subsection 4(1) and is not specified in another instrument made for paragraph 30AB(1)(a) of the Act. The purpose of this is to provide that the CIRMP requirements specific to naval shipbuilding precincts cannot be applied to other critical infrastructure assets, to which Part 2A applies and make clear the responsible entities for those assets are not required to comply with the requirements in the instrument.

Section 6 Relevant Commonwealth Regulator

Section 6 of the instrument specifies, for paragraph (a) of the definition of ***relevant Commonwealth regulator*** in section 5 of the Act, the Department of Defence as the relevant Commonwealth regulator for the critical infrastructure assets mentioned in subsection 4(1) of the instrument.

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 Department of Defence.

Part 2 Requirements for a critical infrastructure risk management program

Section 7 Material risks

Section 7 sets out that, under subsection 30AH(8) of the Act, a '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 section 8 of the instrument (personnel hazards) and any other hazard identified by the responsible entity, such as physical security hazards. The purpose of section 7 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 (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 8 Personnel hazards

Section 8 of the instrument specifies, for paragraph 30AH(1)(c) of the Act, requirements that a CIRMP must comply with.

Subsection 8(1) of the instrument requires a responsible entity, for personnel hazards, to establish and maintain a process or system in a CIRMP:

- to only permit a person unescorted access to a critical infrastructure asset where:
    - a background check of the person has been conducted under the AusCheck scheme (further detail on background check requirements are detailed below) (subparagraph (a)(i)); and

- the person has been found suitable to have unescorted access to the asset (further detail on assessing suitability is detailed below) (subparagraph (a)(ii)); and

- an identity card has been issued to the person who has completed a background check and has been found suitable to have unescorted access (subparagraph (a)(iii)); and

- to collect the identity and contact information for each person who has access to the critical infrastructure asset (paragraph (b))—this information must be recorded regardless of whether the person is permitted to have unescorted access or not; and

- to record the date, time and duration of access to the critical infrastructure asset by any person, escorted or unescorted (paragraph (c)); and

- as far as reasonably practicable to do so—to minimise or eliminate material risks:

  - arising from a malicious or negligent person (subparagraph (d)(i)); and

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

Subsection 8(2) of the instrument provides, for subsection 30AH(12) of the Act, that the establishment and maintenance of a process or system mention in subsection 8(1) is taken to be action that mitigates the relevant impact of risk of personnel hazards on the critical infrastructure asset. 'Relevant impact' of a hazard on a critical infrastructure asset is defined in section 8G of the Act to mean the impact (whether direct or indirect) on the availability, integrity or reliability of the asset; or on the confidentiality of information about the asset, information stored on the asset, or the computer data if the asset is computer data.

Section 9 Background checks

Subsection 9(1) of the instrument provides a background check is required:

- before a person is granted unescorted access to the critical infrastructure asset (paragraph (a)); and

- if a person requires ongoing unescorted access to the critical infrastructure asset—a background check is required every two years (paragraph(b)).

The inclusion of this timeframe will ensure any behaviour, subsequent to the initial background check, is able to be identified and assessed at 2 year intervals, to inform the risk and mitigation plans.

Subsection 9(2) of the instrument, for paragraph 30AH(4)(a) of the Act, provides that the background check must be conducted under the AusCheck scheme.

Subsection 9(3) of the instrument provides that a 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 the AusCheck scheme. This will empower them to consider whether a person is suitable to be permitted unescorted access to the critical infrastructure asset, or determine a suitable mitigation strategy where necessary.

Section 10 Suitability assessment

Subsection 10(1) of the instrument provides that, following a background check under section 9, a responsible entity must assess the suitability of a person to have unescorted access to the critical infrastructure asset.

Subsection 10(2) provides that in making a suitability assessment for subsection (1), a responsible entity must consider:

- any advice from the Secretary of the Department under the following provisions of the AusCheck Regulations: (paragraph (2)(a));
    - paragraph 21DA(2)(a)—whether or not the individual has an unfavourable criminal history (subparagraph (2)(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 (2)(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 (2)(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 (2)(a)(iv)); and
- whether permitting the person unescorted access to a critical infrastructure asset mentioned in subsection 4(1) 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)).

Section 9 of the instrument requires responsible entities to consider the security risk of an individual and provides relevant information to enable them to take steps to control or limit access to the critical infrastructure asset, as required.

The note contained in subsection 10(2) reinforces the purpose of subparagraph 10(2)(a)(ii) by reminding responsible entities of the obligation, under section 21ZA of the AusCheck Regulations, to inform the Secretary of certain decisions the responsible entity takes.

Schedule 1 Naval shipbuilding precinct

1 Osborne Naval Shipyard

Schedule 1 to the instrument includes a map of Osborne Naval Shipyard, which identifies, using different colours, areas of the precinct to which obligations in Part 2A of the Act apply. The obligations will apply if the area is, or an asset within the area is, a critical infrastructure asset, as prescribed in subsection 4(1) of the instrument.

Schedule 1 includes a table which specifies the responsible entity for critical infrastructure assets, within a relevantly identified area of the map. The responsible entity for critical infrastructure assets within an area is the entity that operates in and is responsible for that area.

For example, ASC Shipbuilding Pty Ltd (trading as ‘BAE Systems Maritime Australia) (ABN 15 051 899 864) is responsible for areas of the map coloured red and is specified as the responsible entity for critical infrastructure assets within those areas.

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 (Naval shipbuilding precinct) Rules (LIN 23/007) 2023

This Disallowable Legislative Instrument (the 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 Part 2A of the *Security of Critical Infrastructure Act* 2018 (the SOCI Act) provides that a 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.

2 The purpose of the instrument is to specify requirements for a CIRMP for specified naval shipbuilding assets. The instrument does this by:

- prescribing, for paragraph 9(1)(f) of the Act, that an asset within a naval shipbuilding precinct that is owned or operated by an entity for the purpose of naval shipbuilding and sustainment as a critical infrastructure asset (see further detail in Attachment A);
- prescribing, for subsection 12L(23) of the Act, the responsible entity for the prescribed critical infrastructure asset;
- specifying, for paragraph 30AH(1)(a) of that Act, that Part 2A of the Act applies to the critical infrastructure assets;
- providing, for subsection 30AH(3) of the Act, that Part 2A, including the CIRMP requirements specified in the instrument, apply to the critical infrastructure assets 12 months after the instrument commences;
- specifying the Department of Defence as the ***relevant commonwealth regulator***, for paragraph (a) of that definition in section 5 of the Act, for the critical infrastructure assets; and
- specifying, for paragraph 30AH(1)(c), the requirements that a CIRMP must comply with.

3 The instrument therefore operates to specify that Part 2A of the Act applies to prescribed critical infrastructure assets and the responsible entities for those assets must adopt, maintain and comply with a CIRMP (see sections 30AC and 30AD). The instrument also operates to specify matters which the CIRMP must comply with.

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 collection, use and disclosure of personal information for the purposes of an AusCheck background check is authorised by the *AusCheck Act 2007* (the AusCheck Act) and the *AusCheck Regulations 2017* (the AusCheck Regulations). The *AusCheck Legislation (Critical Infrastructure Background Check) Regulations 2023* amends the AusCheck Regulations to include critical infrastructure background checking within the AusCheck scheme. The instrument requires responsible entities to establish and maintain a process to assess the suitability of a person to have unescorted access to the critical infrastructure asset. The instrument enables the responsible entity to require an AusCheck background check for that purpose.

6 Rules made for the purposes of paragraph 30AH(1)(c) of the SOCI Act seek to minimise the security and economic impact on industry from its ongoing exposure to the risks associated with all hazards. The Disallowable Legislative Instrument, in particular, focuses on personnel hazards. Emerging risks are rapidly outpacing the current regulatory environment.

Human rights implications

The instrument engages the following rights:

- The right to equality and non-discrimination – Article 2(1) and Article 26 of the *International Covenant on Civil and Political Rights* (ICCPR) and Article 2(2) of the *International Covenant on Economic, Social and Cultural Rights* (ICESCR); and

- The right to privacy in Article 17(1) of the ICCPR.

The right to equality and non-discrimination

1 Article 2(1) of the ICCPR and Article 2(2) of the ICESCR provide that the rights in both covenants are to be exercised without discrimination of any kind as to race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status. Similarly, Article 26 of the ICCPR provides that the law shall prohibit any discrimination and guarantee to all persons equal and effective protection against discrimination on any ground such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status.

2 The instrument imposes a requirement on responsible entities to require an AusCheck background check as a condition of having unescorted access to the parts of their facilities designated as critical infrastructure assets. This may result in the responsible entity engaging in differential treatment on the basis of 'other status' (a person's criminal or national security history). To the extent that the AusCheck background check might restrict an employee's unescorted access to the naval shipyard precinct and/or permit the implementation of controls or limit access to the critical infrastructure asset on security grounds which may affect some, but not all, employees, the right to equality and non-discrimination will be engaged. However, any limitation that comes from a responsible entity taking action in response to AusCheck advice about an individual's background check is reasonable, necessary and proportionate. That is because actions taken in response to background checks only

apply to individuals with a 'CIRMP criminal record', an adverse security assessment, or qualified security assessment. A 'CIRMP criminal record' is defined in the AusCheck Regulations to include offences in Schedule 2. In making a suitability assessment of a person to have unescorted access, a responsible entity must also consider whether permitting the person such access would be prejudicial to security. This is the least restrictive means of ensuring that individuals with access to critical infrastructure assets in a naval shipyard do not pose a threat to the security, or operability, of a critical infrastructure asset.

3 Further, a responsible entity does not have a mandatory obligation to take action in response to advice given by AusCheck. Rather, the responsible entity will need to take action in accordance with its CIRMP. This may include ensuring that the individual does not have unescorted access to a critical infrastructure asset, transferring an individual with an identified security risk to the critical infrastructure asset to another part of the business, or terminating the employment of an individual deemed to be too significant a risk to the critical infrastructure asset. To the extent that any action limits the right to freedom from discrimination, any limitation is reasonable and necessary. The impact of security hazards to a naval shipbuilding precinct has the potential to significantly disrupt that infrastructure. It is reasonable and necessary to ensure that personnel risks to those assets are adequately identified and managed, to protect national security.

4 Appropriate safeguards also exist if an individual is issued with an 'unfavourable criminal history'. Section 26 of the AusCheck Regulations provides that a person can seek merits review at the Administrative Appeals Tribunal (AAT) of a decision by the Home Affairs Secretary to advise that an individual has an 'unfavourable criminal history'. The AusCheck Regulations define 'unfavourable criminal history' to include 'CIRMP criminal history' meaning that a person will be able to seek AAT review of advice that the outcome of an AusCheck background check is that they have been found to have an 'unfavourable criminal history'.

5 A review mechanism for an adverse or qualified security assessment is also provided by subsection 27AA(1) of the *Administrative Appeals Tribunal Act 1975*, which states that an application under subsection 54(1) of the *Australian Security Intelligence Organisation Act 1979* (the ASIO Act) for review of a security assessment may be made by a person in respect of whom the assessment was made and who has, in accordance with Part IV of the ASIO Act, been given notice of the assessment.

6 This ensures that to the extent the measures limit the right to non-discrimination, any limitation is not arbitrary, and is reasonable and proportionate.

Right to privacy

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

8 Paragraphs 8(1)(b) and (c) of the instrument engages the right to privacy by requiring responsible entities:

- to collect the identity and contact details for each person who has access to the critical infrastructure asset; and

- record the date, time and duration of access to the critical infrastructure asset by each person.

9 Collection of this information is not limited to the employees or contractors of the responsible entity, but every person who has access to their critical infrastructure asset.

10 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 the defence of Australia. Requiring responsible entities to collect this information helps to ensure that risks to critical infrastructure posed by personnel hazards can be mitigated, as the persons may need to be quickly identified to minimise or eliminate a material risk occurring, such as those specified in section 7 of the instrument. For example, an impairment of the asset that may prejudice the defence of Australia or national security (paragraph 7(b) of the instrument), or a stoppage or major slowdown of the asset's function for an unmanageable period (paragraph 7(c) of the instrument).

11 The instrument also enables a responsible entity to conduct a background check of a person through the AusCheck Act. To the extent that the responsible entity submits a person'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. A background check on a person is necessary as a responsible entity is required to assess the suitability of a person to have unescorted access to the critical infrastructure asset, and must consider whether permitting the person such access would be prejudicial to security. For the purposes of the instrument, security is defined in section 4 of the ASIO Act to relevantly include the protection from espionage, sabotage, attacks on Australia's defence system, and acts of foreign interference.

12 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. To the extent that the 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 the critical infrastructure assets and the role they have for national security and the defence of Australia.

Conclusion

The Disallowable Legislation Instrument is compatible with human rights because to the extent that it may limit human rights, those limitations are reasonable, necessary and proportionate.

The Honourable Clare O'Neil MP
Minister for Home Affairs