

27 November 2023

The Hon Clare O'Neil MP
Minister for Home Affairs
Department of Home Affairs

By email: AusCheck.CI@homeaffairs.gov.au

Dear Minister,

FORMAL CONSULTATION FOR NAVAL SHIPBUILDING (NS) RULE CHANGES

1. On 17 February 2023, the *Security of Critical Infrastructure (Naval shipbuilding precinct) Rules (LIN 23/007) 2023 (the Rules)* commenced, declaring:
 - a. the Osborne Naval Shipyard (**ONS**) as a critical infrastructure asset, for the purpose of the *Security of Critical Infrastructure Act 2018* (Cth) (**SOCI Act**); and
 - b. ASC Shipbuilding Pty Limited trading as BAE Systems Maritime Australia (**BAESMA**) as a responsible entity (**RE**) for certain portions of the ONS.
2. Following numerous engagements with BAESMA and other REs, the Department of Home Affairs (**DHA**) agreed that the drafting of the Rules does not reflect the operational realities of the ONS or the practical outcomes that the Department of Defence (**Regulator**) and DHA (**Governing Bodies**) advised were intended.
3. Following receipt of a copy of the Regulator's Statement of Regulatory Intent (**SORI**), and notice of commencement of formal consultation on the proposed amendments to the Rules (**Amendments**) on 6 November 2023, BAESMA hereby provides its formal submission on the Amendments.
4. On 23 November 2023, the DHA sent an email to BAESMA advising that since the commencement of formal consultation:

ASC Shipbuilding Pty Ltd (trading as BAE Systems Maritime Australia)

ABN 15 051 899 864

Building 01, Level 2, 640 Mersey Road North Osborne SA 5017

baesystems.com.au

- a. the DHA has conducted further engagements with the Regulator, Australian Naval Infrastructure Pty Ltd (**ANI**) and its legal advisors in respect of the Amendments and in respect of the previous queries, issues and proposals submitted by BAESMA prior to the formal consultation commencing; and
 - b. as a result of those further engagements, the DHA has acknowledged issues with the Amendments and invited BAESMA to incorporate some further proposed solutions to remedy such issues.
5. Throughout ongoing consultation over the last few months, the Governing Bodies have repeatedly advised on how they foresee the practical implementation of the Rules will operate, which in BAESMA's view does not align with the drafting contained in the Rules.
6. BAESMA has provided significant feedback and proposed solutions as part of its ongoing collaboration efforts to assist with greater clarity and alignment between the Amendments and the above intent. BAESMA reiterates the key remaining areas of concern which have previously been shared with the Governing Bodies.
7. BAESMA recognises and embraces the importance of protecting Australian Defence assets and is supportive in playing its part to contribute to the achievement of this aim. To that end, clarity in the drafting of the Rules would better achieve the Governing Bodies intent, and support the aim of protecting Australian Defence assets.

Lack of clarity: Perimeter and Scope of RE responsibilities

8. **Issue:** Due to the drafting of the Rules not reflecting the indicated legislative intent, there is lack of clarity on the current perimeter of the ONS to which the Rules apply, and the allocation of responsibilities between REs. Specifically:
 - a. the amended Rules refer to a critical infrastructure asset "within the Osborne Naval Shipyard" but do not confirm the actual perimeter of the ONS captured by the Rules;
 - b. the SORI provides that the Regulator will notify REs "ahead of time (if possible)" where there is a change to the perimeter, however there is no clarity as to the trigger necessitating an update to the perimeter, timeframes allowed to accommodate such change, and any mechanism for inputs by those REs affected. For example, if the area of responsibility for BAESMA expands, sufficient time is required to enable additional background checks to be undertaken;

- c. the SORI and Explanatory Statement both contemplate that the exclusive licence or contractual arrangement referred to in the amended rule 4(1)(c) and rule 4(2)(a) will be with ANI. This, together with the defaulting RE being ANI, infers that ANI is the only possible landlord at the ONS, which does not reflect the operational realities of the ONS because ANI does not own all areas at the ONS, and there are other owners (such as for the Systems Centre);
- d. the amended Rules define an asset as a critical infrastructure asset if it is operated by an entity that has 'exclusive control or usage through licence or other contractual arrangement'. This suggests that any assets operated by their owner or under a non-exclusive arrangement would not fall under the definition of a 'critical infrastructure asset' in rule 4.

9. **Impact:**

- a. The lack of alignment between what we understand to be the Governing Bodies' intent and the drafting of the Rules results in uncertainty for BAESMA as to the extent of its areas of responsibility and impacts on the way in which BAESMA can properly implement processes to ensure full compliance.
- b. The discrepancy between the Rules, the SORI and the Explanatory Statement creates uncertainty as to the intended scope of licences and contractual arrangements for which REs will be responsible under the Rules and gives rise to uncertainty as to whether areas under licence with landlords other than ANI are covered.
- c. The lack of clarity on the definition of a 'critical infrastructure asset' creates uncertainty for REs regarding which areas of the ONS are captured by the Rules and over which areas REs must ensure compliance.

10. **Proposed solution:** The Rules be further amended to provide clarity:

- a. over the boundaries of the perimeter of the ONS that is captured as the 'critical infrastructure asset'. This could be achieved by incorporating **additional** drafting to that currently contained in section 4(1) of the Amendments to clarify a 'critical infrastructure asset' will only be an asset within a clearly delineated perimeter of the ONS precinct, as advised by the Regulator; and
- b. on which assets are to be captured within the definition of a 'critical infrastructure asset'.

BAESMA has reissued proposed drafting for the DHA's consideration – please see Annexure A included with this letter. BAESMA welcomes the opportunity to collaborate with the DHA in respect of that drafting.

Strict compliance of Rules, lack of legal standing of SORI and changing guidance from Regulator

11. **Issue:** While the SORI provides REs with some guidance on how the Rules are intended to be enforced, as previously submitted by BAESMA, the Rules are drafted on a strict compliance basis and the Amendments do not:
 - a. grant any power to the Regulator to permit departure from that strict compliance; or
 - b. provide any legislative power to a guidance document, such as the SORI.
12. For example, while BAESMA appreciates the Regulator is not (currently) making it mandatory for REs to share its suitability assessments with other REs, or for REs to rely on other REs' suitability assessments, BAESMA is concerned with the Regulator providing such advice in the SORI when:
 - a. it does not appear the requirements under the *Privacy Act 1988* (Cth) have been taken into consideration (this was an issue extensively raised in BAESMA's previous correspondence and workshops with the Governing Bodies). For example, REs do not receive the benefit of the approach taken in section 13 of the *AusCheck Act 2007* (Cth); and
 - b. there is no 'carve out' to either the requirement in section 10 of the Rules for REs to conduct their own suitability assessments, or to the liability which the REs may be exposed to if an unsuitable person is granted unescorted access to the area of the ONS for which the RE is responsible.
13. **Further Issue:** During the course of engagement with the Governing Bodies this year, BAESMA has observed changing advice by the Regulator within a short period of time, making it difficult for REs to understand the scope of their responsibilities under the Rules. For example:
 - a. the Governing Bodies advised in previous workshops that all responsibilities in respect of Commonwealth and Navy personnel (i.e., conducting background checks and liability in respect of suitability assessments)

would be 'carved out' from the scope of responsibility of REs, except for those expressly identified by the Regulator;

b. however;

- i. the SORI provides that the Naval Construction Branch, through ANI, and ASC will undertake background checks for all Commonwealth personnel, Navy personnel and Defence-employed contractors; and
- ii. otherwise, REs must still conduct the suitability assessments for Commonwealth and Navy Personnel, for the areas over which they are responsible, notwithstanding advice in the SORI that REs may consider suitability assessments that have been completed by ASC and ANI. This also presupposes that ASC and ANI will share the results of the background checks and their suitability assessments with the other REs, and in its absence, the REs will need to undertake background checks which will result in duplication. This advice presents the same issues described in paragraph 12 above.

14. **Impact:** The practical effects of the SORI not having any legal standing include that:

- a. the issues that the SORI have attempted to rectify (whilst helpful guidance), have not been formally resolved under the Rules and have not granted express exceptions to REs in respect of their obligations; and
- b. if REs follow the guidance in the SORI, the REs will be at risk of being in technical breach of the Rules in the absence of express exceptions or linkage to the SORI. Notwithstanding any recent 'assurances' from the Regulator in the SORI, and verbally, not to enforce the Rules in certain situations, as BAESMA has previously advised the Governing Bodies, the consequences of being in technical breach under the Rules are broader than the financial penalties which may be imposed under the SOCI Act, and may lead to contractual breaches relating to compliance with laws.

15. **Proposed solution:**

a. The Rules be amended to expressly:

- i. permit the Regulator to provide for exceptions to the strict compliance requirements under the

Rules; and

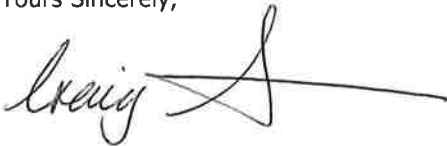
- ii. provide legal standing to the SORI, or otherwise expressly permitting the Regulator to advise in writing of any departures from the Rules.

BAESMA has reissued proposed drafting for the DHA's consideration – please see Annexure A included with this letter. BAESMA welcomes the opportunity to collaborate with the DHA in respect of that drafting.

- b. The Regulator to document and implement a process for updating the SORI, to ensure that REs have sufficient notice to address any changes that may affect their operations.

16. BAESMA appreciates the opportunity to provide this submission, and again expresses its willingness to collaborate on any drafting required to ensure the intention of both the Governing Bodies, and the operational realities of the ONS, are reflected in the next iteration of the Rules.

Yours Sincerely,



Craig Lockhart
Managing Director
BAE Systems Australia - Maritime

Annexure A: Proposed drafting – Amendments to the Rules



LIN 23/007

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

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

Dated 31 January 2023

Clare O’Neil

Minister for Home Affairs

Part 1 Preliminary

1 Name

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

2 Commencement

This instrument commences on the later of:

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

Note For pre-conditions to making this instrument—see Act, sections 30ABA and 30AL.

3 Definitions

Note Some terms used in this instrument are defined in the Act, including:

- (a) asset;
- (b) AusCheck scheme;
- (c) critical infrastructure asset;
- (d) entity;
- (e) relevant impact;
- (f) responsible entity;
- (g) security.

In this instrument:

AusCheck Act means the *AusCheck Act 2007*.

AusCheck Regulations means the *AusCheck Regulations 2017*.

background check means a background check under the AusCheck scheme.

CIRMP is short for critical infrastructure risk management program.

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

criminal history criteria means the assessment of:

- (a) whether the person has a CIRMP criminal record; and
- (b) the nature of the offence.

Department of Defence means the Department administered by the Minister administering the *Defence Act 1903*.

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

- (a) to compromise the proper function of the asset; or
- (b) to cause significant damage to the asset.

4 Critical infrastructure asset

- (1) For paragraph 9(1)(f) of the Act, an asset is a critical infrastructure asset if it is:
 - (a) located within the Osborne Naval Shipyard precinct, as advised in writing by the relevant Commonwealth Regulator, which is located on the Lefevre Peninsula, South Australia; and
 - (b) used for the primary purposes of naval shipbuilding and sustainment; ~~and~~

- (c) ~~operated by an entity that has been granted exclusive control and usage, through licence or other contractual arrangement, of the asset or the area where the asset is located, for the purpose mentioned in paragraph (b).~~

(2) For the purpose of subsection 4(1)(a), the relevant Commonwealth Regulator shall:

- (a) maintain a map delineating the perimeter of the Osborne Naval Shipyard, which shall be accessible to responsible entities at all times;
- (b) provide notice in writing to the responsible entities of any proposed change to the perimeter of the Osborne Naval Shipyard, allowing the responsible entities sufficient opportunity to ensure compliance with the Act and these Rules in respect of any expansion to the perimeter.

(3) For subsection 12L(23) of the Act, the responsible entity for a critical infrastructure asset mentioned in subsection (1) is:

- (a) an entity that has been granted exclusive control and usage, through licence or other contractual arrangement, of the asset or the area where the asset is located; or
- (b) in all other circumstances, the owner of the asset, including Australian Naval Infrastructure Pty Ltd (ABN 45 051 762 639).

5 Application of Part 2A of the Act

- (1) For paragraph 30AB(1)(a) of the Act, Part 2A of the Act applies to a critical infrastructure asset mentioned in subsection 4(1).
- (2) For subsection 30AB(3) of the Act, Part 2A of the Act applies to a critical infrastructure asset mentioned in subsection 4(1), 12 months after the asset becomes a critical infrastructure asset.
- (3) The requirements specified in this instrument for paragraph 30AH(1)(c) of the Act apply to a critical infrastructure asset that:
 - (a) is mentioned in subsection 4(1); and
 - (b) is not specified in another instrument for paragraph 30AB(1)(a) of the Act.

6 Relevant Commonwealth Regulator

For paragraph (a) of the definition of *relevant Commonwealth regulator* in section 5 of the Act, the Department of Defence is specified for a critical infrastructure asset mentioned in subsection 4(1).

Part 2 Requirements for a critical infrastructure risk management program

7 Material risks

For subsection 30AH(8) of the Act, the material risks include the following:

- (a) a stoppage or major slowdown of the critical infrastructure asset's function for an unmanageable period;
- (b) a substantive loss of access to, or deliberate or accidental manipulation of, a critical component of the critical infrastructure asset;

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

- (c) an interference with the critical infrastructure asset's operation technology or information communication technology essential to the functioning of the asset;

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

- (d) the storage, transmission or processing of sensitive operational information outside Australia, which includes:
 - (i) layout diagrams;
 - (ii) schematics;
 - (iii) geospatial information;
 - (iv) configuration information;
 - (v) operational constraints or tolerances information;
 - (vi) data that a reasonable person would consider to be confidential or sensitive about the asset;
- (e) remote access to operational control or operational monitoring systems of the critical infrastructure asset.

8 Personnel hazards

- (1) For paragraph 30AH(1)(c) of the Act, for personnel hazards, a responsible entity must establish and maintain a process or system in a CIRMP:
 - (a) to permit a person unescorted access to a critical infrastructure asset mentioned in subsection 4(1) only where:
 - (i) a background check of the person has been conducted in accordance with section 9; and
 - (ii) a person has been found suitable to have unescorted access to the critical infrastructure asset in accordance with section 10; and
 - (iii) an identity card has been issued to a person who meets the requirements in subparagraphs (i) and (ii); and
 - (b) to collect the identity and contact information for each person who has access to the critical infrastructure asset; and
 - (c) to record the date, time and duration of access to the critical infrastructure asset by each person; and
 - (d) as far as it is reasonably practicable to do so—to minimise or eliminate material risks:
 - (i) arising from a malicious or negligent person; and
 - (ii) arising from the off-boarding process for outgoing employees and contractors.

- (2) For subsection 30AH(12) of the Act, the establishment and maintenance of processes or systems mentioned in subsection (1) is taken to be action that mitigates the relevant impact of personnel hazards on the critical infrastructure asset.

9 Background checks

- (1) Except where the relevant Commonwealth Regulator advises otherwise in writing, a background check is required:
 - (a) before a person is granted unescorted access to the critical infrastructure asset; and
 - (b) if the person requires ongoing access to the critical infrastructure asset—every 2 years.
- (2) For paragraph 30AH(4)(a) of the Act, a background check of a person must be conducted under the AusCheck scheme.
- (3) A background check must include an assessment of information relating to the matters mentioned in paragraphs 5(a), (b), (c) and (d) of the AusCheck Act; and
 - (a) for paragraph 30H(4)(c) of the Act—the criteria against which the information must be assessed are the criminal history criteria; and
 - (b) for paragraph 30AH(4)(d) of the Act—the assessment must consist of both an electronic identity verification check and an in person identity verification check.
- (4) A responsible entity must notify the Secretary if a background check is no longer required for a person.

10 Suitability assessment

- (1) Following a background check under section 9, except where the relevant Commonwealth Regulator advises otherwise in writing, a responsible entity must assess the suitability of a person to have unescorted access to the critical infrastructure asset.
- (2) In making a suitability assessment for subsection (1), a responsible entity must consider:
 - (a) any advice from the Secretary under the following provisions of the AusCheck Regulations:
 - (i) paragraph 21DA(2)(a);
 - (ii) paragraph 21DA(2)(b);
 - (iii) subsection 21DA(4);
 - (iv) subsection 21DA(5); and
 - (b) whether permitting the person unescorted access to a critical infrastructure asset mentioned in subsection 4(1) would be prejudicial to security; and
 - (c) any other information that may affect the person's suitability to have unescorted access to the asset.

Note A responsible entity may be required to inform the Secretary of a decision to grant or revoke access to a critical infrastructure asset, in certain circumstances—see AusCheck Regulations, section 21ZA.

