



Australian Government
Department of Home Affairs

Submission

For decision

PDMS Ref. Number: MS24-001415

Date of Clearance: 4/9/2024

To Minister for Home Affairs

Subject Declarations of Systems of National Significance under the Security of Critical Infrastructure Act 2018 – s. 33(a)(i)

Timing For consideration by 7 October 2024.

Recommendations

That you:

1. **note** that the Department of Home Affairs (the Department) has facilitated mandatory consultation with responsible entities on the proposed declaration of their critical infrastructure assets as Systems of National Significance (SoNS); noted / please discuss
2. in accordance with the legislative requirement that you consider submissions made by responsible entities, **note** that you have s. 33(a)(i) noted / please discuss
3. in accordance with paragraphs 13 to 16, **agree** to declare the s. 33(a)(i) agreed / not agreed
4. in accordance with paragraphs 17 (and 22 to 24), **agree** to s. 33(a)(i); agreed/ not agreed
5. if you agree to recommendation 3 and 4, **sign and date** the: signed / not signed
 - a. s. 33(a)(i)

Released by Department of Home Affairs
under the Freedom of Information Act 1982

6. in accordance with paragraph 20, s. 33(a)(i)

[REDACTED]

agreed and signed / not
agreed

7. s. 33(a)(i), s. 47E(d)

[REDACTED]

noted / please discuss

Minister for Home Affairs

Signature.....

Date:...../...../2024

Released by Department of Home Affairs
under the Freedom of Information Act 1982

Minister's Comments

Key Issues

1. As the Minister for Home Affairs, you may declare critical infrastructure assets as Systems of National Significance (SoNS) under section 52B of the *Security of Critical Infrastructure Act 2018* (SOCI Act).

2. This submission seeks your agreement to s. 33(a)(i)

3. SoNS are a smaller subset of critical infrastructure assets that are most crucial to the nation, by virtue of their interdependencies across sectors and potential for cascading consequences to other critical infrastructure assets and sectors if disrupted. SoNS have been identified through whole of economy analysis and research conducted by the Department of Home Affairs (the Department) (s. 33(a)(i)) and in consultation with the states and territories and other commonwealth departments, agencies and regulators.

4. s. 33(a)(i)

5. Should you declare these additional assets, s. 33(a)(i)

6. The list of SoNS is not publicly available. Information that records the fact that an asset is a SoNS is protected information under the SOCI Act. An entity commits an offence if they disclose this information, unless authorised under Part 4 of the SOCI Act.

s. 33(a)(i)

7. The SOCI Act requires that, before making a declaration, the Minister must give the responsible entity a notice setting out the proposed declaration and inviting submissions.

8. On 29 May 2024, the former Minister agreed to commence mandatory consultation in relation to s. 33(a)(i), s. 47E(d)

9. s. 33(a)(i)

10. Consultation consisted of:

- three town-hall-style information sessions hosted by the Department;
- individual bilateral meetings between the Department and the responsible entities;
- review of the draft statement of reasons; and
- an invitation to provide a written submission in response to the proposed declaration and statement of reasons.

11. s. 33(a)(i)

12. In accordance with section 52C of the SOCI Act, you must consider submissions received during the consultation period before making or amending a declaration.

s. 33(a)(i)

13. As consultation has now taken place, you may declare these critical infrastructure assets to be SoNS if you are satisfied they are of national significance.

14. In determining whether an asset is of national significance, you must have regard to:

- the consequences that would arise for the social and economic stability of Australia or its people, or the national security or defence of Australia if a hazard were to occur that had a significant relevant impact on the asset (that being the availability, integrity or reliability of the asset, or on the confidentiality of information); and
- if you are aware of one or more interdependencies between the asset and one or more other critical infrastructure assets – the nature and extent of those interdependencies and
- such other matters (if any) that you consider relevant.

s. 33(a)(i)

s. 33(a)(i)

18. Should you agree to make these new declarations and s. 33(a)(i) [REDACTED], you must:

- Sign and date the s. 33(a)(i) [REDACTED]
- sign and date the s. 33(a)(i) [REDACTED]

Released by Department of Home Affairs
under the Freedom of Information Act 1982

PROTECTED

- sign the s. 33(a)(i)

19. Under subsection 52B(3) of the SOCI Act, you must also notify: direct interest holders in relation to the assets, the Parliamentary Joint Committee on Intelligence and Security (PJCIS), and First Ministers where the declarations relate to assets either wholly or partly in their jurisdiction. If you agree to the declarations:

- sign and date the s. 33(a)(i)

- sign and date the s. 33(a)(i)

- sign and date the s. 33(a)(i)

20. s. 33(a)(i)

s. 33(a)(i)

[REDACTED]

[REDACTED]

[REDACTED]

Background

Enhanced Cyber Security Obligations

25. Once an asset has been declared a SoNS, responsible entities may be subject to Enhanced Cyber Security Obligations under Part 2C of the SOCI Act. There are four Enhanced Cyber Security Obligations:

- adopt, comply with, review and update an **incident response plan** to prepare for a cyber security incident;
- undertake a **cyber security exercise** to build cyber preparedness;
- undertake **vulnerability assessments** to identify vulnerabilities for remediation; and
- Provide **system information** to develop and maintain a near-real time threat picture.

26.s. 33(a)(i)

[REDACTED]

27. Enhanced Cyber Security Obligations are not automatically applied to a SoNS asset, rather, they are enlivened by a written notice given to the responsible entity, following a period of consultation.

28. The power to apply the Enhanced Cyber Security Obligations is held by the Secretary (or a delegate). s. 33(a)(i)

[REDACTED]

[REDACTED]

29. In addition to the Enhanced Cyber Security Obligations regulatory framework, the Department places significant emphasis on developing a genuine partnership with the SoNS entities to support cyber security uplift.

Released by Department of Home Affairs
under the Freedom of Information Act 1982

30. s. 33(a)(i)



32. s. 33(a)(i), s. 47E(d)



33. s. 33(a)(i)



Consultation – internal/external

34. Internal – s. 47E(d).

35. External – s. 33(a)(i), s. 47E(d)



Consultation – Secretary

37. The Secretary has not been consulted on this submission.

Client service implications

38. Nil.

Risks and Sensitivities

39. Information that records or is the fact that an asset has been declared under section 52B of the SOCI Act to be SoNS is protected information and must be handled in accordance with Part 4 of the SOCI Act.

Financial/systems/legislation/deregulation/media implications

40. A media release will be provided to your office via the Department's media team.

41. The information contained in this submission is classified and should not be publicly released without the authority of the Department of Home Affairs. In accordance with our long standing practices, should you wish for unclassified media lines to be prepared in relation to this issue please contact the Home Affairs Media team – ^{s. 22(1)(a)(ii)} @homeaffairs.gov.au.

Attachments

S. 33(a)(i)

Authorising Officer

Cleared by:

Cleared electronically

Hamish Hansford
Deputy Secretary
Cyber and Infrastructure Security Group

Date: 04/09/2024

Mob: ^{s. 22(1)(a)(ii)} | T: ^{s. 22(1)(a)(ii)}

Contact Officer: Sally Pfeiffer, First Assistant Secretary, Industry Partnerships and Infrastructure Policy Division,
^{s. 22(1)(a)(ii)} @homeaffairs.gov.au | ^{s. 22(1)(a)(ii)}

CC

Secretary
Deputy Secretary, Executive Group
Deputy Secretary, National Security and Resilience Group
Group Manager, Legal
National Cyber Security Coordinator
Director-General of Security, Australian Security Intelligence Organisation
Head, Australian Cyber Security Centre, Australian Signals Directorate

Released by Department of Home Affairs
under the Freedom of Information Act 1982