



Australian Government
Department of Home Affairs

Submission

For decision

PDMS Ref. Number: MS24-001663

Date of Clearance: 12/09/2024

To **Minister for Home Affairs, Minister for Immigration and Multicultural Affairs, Minister for Cyber Security**

Subject **Systems of National Significance – Review of Declaration –** s. 33(a)(i)
s. 33(a)(i)

Timing By 8 November 2024

Recommendations

That you:

1. **note** Deputy Secretary Cyber and Infrastructure Group (as a delegate of the Secretary) has S. 33(a)(i), s. 47E(d) noted / please discuss

2. **s. 33(a)(i), s. 47E(d)** noted / please discuss

3. **s. 33(a)(i)** signed / not signed

Minister for Home Affairs, Minister for Immigration and Multicultural Affairs, Minister for Cyber Security

Signature.....

Date: / / 2024

Minister's Comments

Key Issues

1. As the Minister for Home Affairs, you have the power under section 52B of the *Security of Critical Infrastructure Act 2018* (the SOCI Act) to privately declare a critical infrastructure asset to be a System of National Significance (SoNS).
2. Under section 52E of the SOCI Act, a responsible entity for a SoNS can request the Secretary to review the SoNS declaration, that is, to review whether the asset is of national significance.

s. 33(a)(i)

3.

s. 33(a)(i)

s. 33(a)(i)

4. s. 33(a)(i) the former Minister for Home Affairs (the Hon Clare O'Neil MP) declared the following s. 33(a)(i) assets to be SoNS.

• s. 33(a)(i)

5.

s. 33(a)(i)

6.

s. 33(a)(i)

7. Deputy Secretary Cyber and Infrastructure Security Group, Hamish Hansford, as a delegate of the Secretary in accordance with section 59 of the SOCI Act, s. 33(a)(i)

s. 33(a)(i)

8. s. 33(a)(i)

9. s. 33(a)(i)

s. 33(a)(i)

10. s. 33(a)(i)

11. s. 33(a)(i)

Background

12. 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.

13. 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.

14. These Enhanced Cyber Security Obligations are additional to any existing positive security obligations that apply to a particular SoNS asset under the SOCI Act. For example, s. 33(a)(i)

15. s. 33(a)(i)

16. s. 33(a)(i)

This submission also provided an overview on the application of the Enhanced Cyber Security Obligations and the in-person and online engagement activities facilitated through the s. 33(a)(i) See s. 33(a)(i) for the list of proposed SoNS to be declared as part of s. 33(a)(i)

Consultation – internal/external

17. Internal – Legal Group.

18. s. 33(a)(i)

Consultation – Secretary

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

Client service implications

20. Nil.

Risks and Sensitivities

21. Information that records or includes 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 Act.

Financial/systems/legislation/deregulation/media implications

22. 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 Coordination team – media@homeaffairs.gov.au.

s. 33(a)(i)

Authorising Officer

Cleared by:

s. 22(1)(a)(ii)

Hamish Hansford
Deputy Secretary
Cyber and Infrastructure Security Group

Date: 12/09/2024

M: s. 22(1)(a)(ii) | T: s. 22(1)(a)(ii)

Contact Officer: Sally Pfeiffer, First Assistant Secretary – Critical Infrastructure Partnerships and Policy
Division, s. 22(1)(a)(ii)@homeaffairs.gov.au | s. 22(1)(a)(ii) or s. 22(1)(a)(ii)

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

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