Security of Critical Infrastructure (Critical infrastructure risk management program) Amendment (Data Storage Systems) Rules 2024

I, Tony Burke, Minister for Home Affairs and Minister for Cyber Security, make the following rules.

Dated 2024

Tony Burke **EXPOSURE DRAFT ONLY—NOT FOR SIGNATURE**
Minister for Home Affairs
Minister for Cyber Security

EXPOSURE DRAFT ONLY

Contents

1 Name 1
2 Commencement 1
3 Authority 1
4 Schedules 1

Schedule 1—Amendments **2**

EXPOSURE DRAFT ONLY

1 Name

This instrument is the *Security of Critical Infrastructure (Critical infrastructure risk management program) Amendment (Data Storage Systems) Rules 2024*.

2 Commencement

This instrument commences on the later of:

(a) the day after this instrument is registered; and

(b) immediately after the commencement of Parts 1 and 2 of Schedule 5 to the *Security of Critical Infrastructure and Other Legislation Amendment (Enhanced Response and Prevention) Act 2024*.

3 Authority

This instrument is made under section 61 of the *Security of Critical Infrastructure Act 2018*.

4 Schedules

Each instrument that is specified in a Schedule to this instrument is amended or repealed as set out in the applicable items in the Schedule concerned, and any other item in a Schedule to this instrument has effect according to its terms.

EXPOSURE DRAFT ONLY

Schedule 1—Amendments

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

1 Section 3 (note)

Repeal the note, substitute:

Note A number of expressions used in this instrument are defined in the Act, including:
(a) business critical data;
(b) critical component;
(c) critical infrastructure asset;
(d) critical hospital;
(e) critical worker;
(f) relevant impact;
(g) responsible entity;
(h) security.

2 Section 3

Insert:

Act means the *Security of Critical Infrastructure Act 2018*.

3 At the end of subsection 4(1)

Insert:

Note A data storage system that satisfies all of the requirements under subsection 9(7) of the Act in respect of a critical infrastructure asset specified in subsection (1) is taken to be part of the critical infrastructure asset.

4 After subsection 4(3)

Insert:

Compliance with Part 2A obligations through other instruments

(4) If:
(a) an entity is the responsible entity for a CI asset specified in subsection 4(1) (***CIRMP asset***); and
(b) that entity is also the responsible entity for another CI asset that is specified in another instrument for the purposes of paragraph 30AB(1)(a) of the Act (***other asset***); and
(c) a CIRMP that applies to the entity for the CIRMP asset complies with the requirements specified for paragraph 30AH(1)(c) in the other instrument relating to the other asset (as if those requirements relate to the CIRMP asset); and
(d) the entity complies with the requirements specified for subsections 30AKA(1),(3) and (5) in the other instrument;

then the requirements that apply to the CIRMP and the entity, and specified for paragraph 30AH(1)(c) and subsections 30AKA(1), (3) and (5) in this instrument, are taken to be complied with.

Example: An entity is a responsible entity for 2 assets—a critical broadcasting asset and a relevant critical infrastructure asset. The relevant critical infrastructure asset is

EXPOSURE DRAFT ONLY

specified in another instrument. The entity applies the requirements in the other instrument to its critical broadcasting asset as if the critical broadcasting asset is a relevant critical infrastructure asset. If the entity complies with the requirements in the other instrument for both assets, it is taken to have complied with the requirements in this instrument.

5 At the end of section 6

Add:

; (f) impact to the availability, integrity, reliability or confidentiality of the data storage system holding business critical data.

EXPOSURE DRAFT ONLY