EXPOSURE DRAFT

Cyber Security (Ransomware Reporting) Rules 2024

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

Dated 2024

Tony Burke **[DRAFT ONLY—NOT FOR SIGNATURE]**
Minister for Home Affairs

Contents

Part 1—Preliminary

1 Name

This instrument is the *Cyber Security (Ransomware Reporting) Rules 2024*.

2 Commencement

(1) Each provision of this instrument specified in column 1 of the table commences, or is taken to have commenced, in accordance with column 2 of the table. Any other statement in column 2 has effect according to its terms.

Commencement information		
Column 1	**Column 2**	**Column 3**
Provisions	**Commencement**	**Date/Details**
1. The whole of this instrument	The later of: (a) at the start of the day after this instrument is registered; and (b) at the same time as Part 3 of the *Cyber Security Act 2024* commences.	

Note: This table relates only to the provisions of this instrument as originally made. It will not be amended to deal with any later amendments of this instrument.

(2) Any information in column 3 of the table is not part of this instrument. Information may be inserted in this column, or information in it may be edited, in any published version of this instrument.

3 Authority

This instrument is made under the *Cyber Security Act 2024*.

4 Definitions

Note: A number of expressions used in this instrument are defined in the Act, including the following:
(a) cyber security incident;
(b) ransomware payment;
(c) reporting business entity.

In this instrument:

Act means the *Cyber Security Act 2024*.

Part 2—Ransomware reporting obligations

5 Simplified outline of this Part

Part 3 of the Act imposes an obligation to provide a ransomware payment report if an entity:

(a) is a reporting business entity; and

(b) is impacted by a cyber security incident; and

(c) has provided, or is aware that another entity has provided on their behalf, a ransomware payment to an entity that is seeking to benefit from the impact or the cyber security incident.

Generally an entity will only be a reporting business entity if it:

(a) is a responsible entity for a critical infrastructure asset to which Part 2B of the *Security of Critical Infrastructure Act 2018* applies; or

(b) is carrying on a business in Australia with an annual turnover for the previous financial year that exceeds the turnover threshold (see section 6) for that year.

Particular information must be included in a ransomware payment report, including information relating to the cyber security incident, the demand made by the extorting entity and the ransomware payment. The information contained in the report must be in accordance with the requirements provided by the rules (see section 7).

6 Turnover threshold

(1) For the purposes of paragraph 26(3)(b) of the Act, the amount of turnover threshold for a business for the previous financial year is $3 million.

(2) For the purposes of paragraph 26(3)(a) of the Act, if a business has been carried on for only part of the previous financial year, the turnover threshold for the business for the previous financial year is worked out using the formula:

$$\$3\text{ million} \times \frac{\text{Number of days in the part}}{\text{Number of days in the previous financial year}}$$

7 Requirements for information that ransomware payment report must contain

(1) For the purposes of subsection 27(2) of the Act, this section prescribes requirements for information that a ransomware payment report given by a reporting business entity must contain.

Note: Information is only required to be given to the extent that the reporting business entity knows or is able, by reasonable search or enquiry, to find out within the 72 hour time period for giving the report.

(2) The reporting business entity's contact and business details given for the purposes of paragraph 27(2)(a) of the Act must include the entity's ABN (if any) and address.

(3) The other entity's contact and business details given for the purposes of paragraph 27(2)(b) of the Act must include the entity's ABN (if any) and address.

(4) The information about the cyber security incident, including its impact on the reporting business entity, given for the purposes of paragraph 27(2)(c) of the Act must include the following:

(a) when the incident occurred or is estimated to have occurred;

(b) when the reporting business entity became aware of the incident;

(c) the impact of the incident on the reporting business entity's infrastructure;

(d) the impact of the incident on the reporting business entity's customers; and

(e) what variants (if any) of ransomware or other malware were used;

(f) what vulnerabilities (if any) in the reporting business entity's system were exploited;

(g) information that could assist the response to, mitigation or resolution of the cyber security incident by a Commonwealth body or State body.

Note: Ransomware payment reports may only be used or disclosed for permitted purposes which include purposes relating to the response to, mitigation or resolution of the cyber security incident. The information must not be disclosed to a State body unless a Minister of the State or Territory has consented: see section 11 of the Act.

(5) The information about the demand made by the extorting entity given for the purposes of paragraph 27(2)(d) of the Act must include:

(a) the amount or quantum of the payment demand; and

(b) the method of payment demanded.

(6) The information about the ransomware payment given for the purposes of paragraph 27(2)(e) of the Act must include:

(a) the amount or quantum of the payment; and

(b) the method of payment.

(7) The information about communications with the extorting entity relating to the incident, the demand and the payment given for the purposes of paragraph 27(2)(f) of the Act must include:

(a) the nature and timing of any communications between the entity and the extorting entity; and

(b) a brief description of those communications (if any); and

(c) a brief description of any pre-payment negotiations undertaken in relation to the demand or payment.