Australian Government

Department of Home Affairs

Cyber Security Legislative Reforms – Explanatory Document

Cyber Security (Ransomware Reporting) Rules

Contact us

Enquiries regarding the licence and any use of this document are welcome at:

Department of Home Affairs
PO Box 25
BELCONNEN ACT 2616

P-23-02503-c

Context

Australia's cyber security landscape is evolving quickly, with malicious activities targeting Australia becoming more frequent and sophisticated. The *Cyber Security Act 2024* (Cyber Security Act) is designed to provide a clear legislative framework for broad, whole-of-economy cyber security issues, positioning the Australian Government to respond to new and emerging cyber security threats. The Bill is intended to provide additional protections to Australian citizens and businesses, build mitigations for extant cyber risks, and improve the Government's threat picture to inform protections, incident response procedures, and future policy.

Ransomware remains one of the most destructive types of cybercrime in Australia, crippling digital infrastructure through the encryption of devices, files and folders, rendering essential computer systems inaccessible or inoperable. Cybercriminals often infiltrate commercially sensitive or personal data from victims, threatening the sale or release if ransom demands are not met.

The Government has no mechanism through existing mandatory reporting regimes, such as the *Security of Critical Infrastructure Act 2018*, to gather clear intelligence on the extent and impact of the ransomware threat on Australian businesses. Current voluntary reporting mechanisms remain underutilised and consequently, many ransomware attacks remain significantly underreported.

The Cyber Security Act establishes an obligation for a reporting business entity to provide a ransomware payment report to the Department of Home Affairs and Australian Signals Directorate (ASD).

Turnover threshold

The Cyber Security Act establishes a rule making power for the Minister for Cyber Security, to prescribe the annual turnover threshold for a business, which if earned in the previous financial year, would ensure they are captured by the mandatory ransomware reporting obligation. It is proposed, in the rules, this turnover threshold would be specified at AUD $3 million.

The $3 million threshold was supported by a majority of stakeholders during rounds of consultation in early 2024, and aligns with the *Privacy Act 1988*, where entities with an annual turnover of less than $3 million are considered to be small businesses and exempt from reporting requirements of notifiable data breaches. This does not directly reference the Privacy Act and does not carry the same series of exclusions as provided in the Privacy Act. Should the relevant threshold be amended in the Privacy Act, this threshold will not be impacted.

The selection of this threshold captures approximately 6.56% of registered Australian businesses. This threshold would provide the best balance of regulatory impact versus reporting burden on industry and provide the Australian Government with enhanced visibility and understanding of the ransomware threat and impact.

The Cyber Security Act also establishes a rule making power for the Minister for Cyber Security to specify a formula that applies if a business has been carried on for only part of the previous financial year (to determine their turnover, and whether or not they are captured by the turnover threshold). In the rules, this formula includes the figure '$3 million' multiplied by the number of days in the part, divided by the number of days in the previous financial year. For example, if a business was established in January of a year, and has been operating for 6 months (until the new financial year), the business will use this formula to determine their annual turnover threshold. If this threshold is less than $3 million, the business is not captured by the mandatory ransomware reporting obligation. If this threshold is more than $3 million, the business is captured by the mandatory ransomware reporting obligation.

Information that must be included in reports

The Cyber Security Act establishes a rule making power for the Minister for Cyber Security to provide additional clarity about the specific information that must be included in a ransomware payment report. The core detail of what must be included in a ransomware payment report is outlined in section 27 of the Cyber Security Act.

Information about the reporting entity

The rules specify that where an entity is providing contact and business details, as part of that element it must ensure that it provides its Australian Business Number (if it has one) and address. This address can be its registered business address, head office, primary operations or some other address that can be used to identify the entity, whichever is most appropriate for that entity.

Information about the cyber security incident

Section 27(2)(c) of the Cyber Security Act requires reporting business entities to provide information relating to the cyber security incident, including its impact on the reporting business entity. The rules outline the specific information that must be provided under this requirement:

- when the incident occurred or is estimated to have occurred;
- when the reporting business entity became aware of the incident;

- the impact of the incident on the reporting business entity's infrastructure;
- the impact of the incident on the reporting business entity's customers;
- what variant of ransomware, or malware (if any) was used;
- what vulnerabilities (if any) in the reporting business entity's system were exploited
- information that could assist the response to, mitigation or resolution of the cyber security incident by a Commonwealth body or State body.

There is also a requirement to provide information that would be useful to assist in incident response, mitigation or resolution. This requirement is seeking specific information (if it exists at all) that would provide a tangible benefit to Commonwealth, State and Territory entities in remediating an incident. This information will provide significant value to building Australia's threat picture of ransomware and cyber extortion incidents in Australia. This includes building an understanding of the time differential between when incidents occur and when entities become aware of these incidents, understanding the impact on infrastructure and customers and better understanding the threat vector.

Information about the demand, payment and communications

Section 27 of the Cyber Security Act requires reporting business entities to provide information in relation to the demand made by an extorting entity, the ransomware payment made and communications with the extorting entity relating to the incident, the demand and the payment.

The rules provide necessary clarity to each of these requirements. Where an entity provides information about the demand they received and payment made, they must ensure to include the amount or quantum of that demand and payment, and the method of that demand and payment. For example, where an entity receives a demand for a transfer of 10 units of a crypto currency to a specific crypto currency wallet, all of the number of units, the type of currency and the method of transfer must be reported.

The rules also clarify that information about communications with the extorting entities must include the nature and timing of any communications and any pre-payment negotiations undertaken in relation to the demand or payment. It also requires details of the substance of these communications. This information may be vital to identifying and understanding the threat actor. This would include (with relevant timestamps) a description of all emails, communications across any messaging platform, audio calls and any other communications with the entity, including specifically a description of all pre-payment negotiations.

Reasonable search or inquiry

A reporting business entity may not know or be aware of all details of a cyber security incident at the time of reporting. This is acknowledged in the Cyber Security Act under subsection 27(2) which states that an entity is only required to report information "the entity knows or is able, by reasonable search or inquiry, to find out." It is also not necessary to provide updates to ransomware payment reports that have been provided. This is designed to lessen the regulatory burden on a reporting business entity which is already under stress due to a cyber security incident.

By enabling clarity in the rules, reporting business entities can be certain about what information is required to satisfy the reporting requirements. This also enables flexibility to add new information as technology develops, or to remove information that is no longer helpful.

/