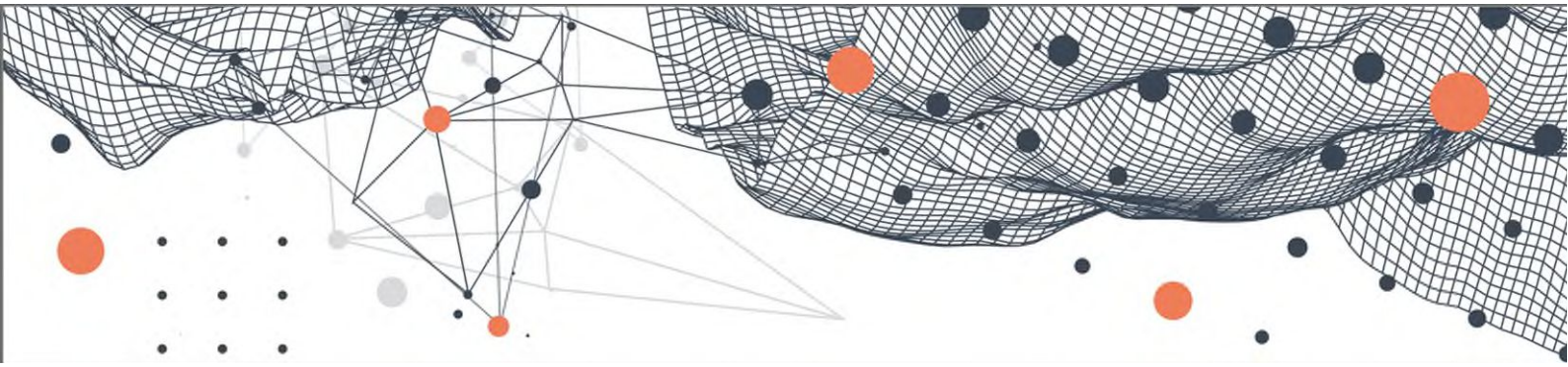

FACTSHEET:

Mandatory ransomware and cyber extortion payment reporting is active from 30 May 2025

What are my obligations under the ransomware and cyber extortion reporting regime?

If you are a **reporting business entity** as defined under Part 3 of the *Cyber Security Act 2024*, you have an obligation to make a report using the reporting form on the Australian Signals Directorate's (ASD) website at https://www.cyber.gov.au/report-and-recover/report when you make a ransomware or cyber extortion payment, or you are aware a payment has been made on your behalf, **within 72 hours of making that payment**.

Section 6 of the Cyber Security (Ransomware Payment Reporting) Rules 2025 (the Rules) specify the annual turnover threshold at AUD $3 million, meaning if your business has an annual turnover of $3 million or more within the last financial year, you are captured by the legislation, and you have a responsibility to report to the Government.

If you have only carried on business for part of a financial year, you must use the formula in section 6 of the rules to determine your annual turnover threshold. This formula is $3 million, times the number of days in the part in the previous financial year, divided by the number of days in the previous financial year.

Case Study

Caolan established a biotechnology start-up, **Biotechnology Solutions**, 73 days before the end of the last financial year. During that time, **Biotechnology Solutions'** annual turnover was $1.2 million. The threshold that applies to Caolan's business would be calculated as follows:

$$\$3\ million \times \frac{Number\ of\ days\ in\ the\ part}{Number\ of\ days\ in\ the\ previous\ financial\ year} = \$3\ million \times \frac{73}{365} = \$600{,}000$$

As the annual turnover threshold that applies to Caolan's business is $600,000, **Biotechnology Solutions** would be considered a reporting business entity for the purposes of the Part.

Entities that are the **responsible entities** for critical infrastructure assets to which Part 2B of the *Security of Critical Infrastructure Act 2018* applies are **reporting business entities** and have a responsibility to report to the Government.

The legislation captures *both* **monetary** and **non-monetary benefits** that are given or exchanged to an extorting entity as being **ransomware or cyber extortion payments**. For example, this may include the exchange of gifts, services or other benefits to an entity in respect of the demand.

What are the roles of the Australian Signals Directorate and the Department of Home Affairs?

The Department of Home Affairs (the Department) administers the *Cyber Security Act 2024* which includes monitoring compliance with the obligation to report ransomware and cyber extortion payments. Where necessary and appropriate, the Department will exercise powers under the *Regulatory Powers (Standard Provisions) Act 2014* with respect to the *Cyber Security Act 2024*.

Under section 8 of the *Cyber Security Act 2024*, the ASD is a 'designated Commonwealth body' and may receive ransomware payment reports. The ASD does not serve as a regulator, and will not monitor compliance with the obligation to report ransomware and cyber extortion payments, or exercise powers under the *Regulatory Powers (Standard Provisions) Act 2014*.

The ASD may receive information contained in a ransomware payment report for the purposes of assisting the reporting business entity to respond to, mitigate or resolve a cyber security incident, or to perform its functions as an intelligence agency. The ASD will not use or disclose ransomware payment information for any other purpose.

When do these reporting obligations come into force?

Part 3 of the *Cyber Security Act 2024,* which sets out the mandatory ransomware and cyber extortion reporting regime, commences **on 30 May 2025**. From this date, all reporting business entities are required to commence ransomware and cyber extortion reporting using the form on ASD's webpage found on: https://www.cyber.gov.au/report-and-recover/report/ransomware-payment-and-cyber-extortion-payment-reporting.

The Department understands that reporting business entities must adapt business practices and processes to accommodate this mandatory reporting obligation, and that there will be a period of transition and familiarisation that occurs as the reporting regime matures.

Implementation of the ransomware payment reporting obligation will occur in two stages:

1. **Phase 1: Education First Approach (30 May 2025 to 31 December 2025, 6 months)** - The Department will prioritise an education-first approach period for the first 6 months after commencement, to socialise the reporting form with regulated entities, manage any challenges and identify key compliance barriers. During this phase, the Department would aim to pursue regulatory action only in cases of egregious non-compliance against businesses that report on incidents, to not take capacity away from impacted entities during the initial incident response phase. The Department will engage with Australian entities, industry groups, peak bodies, and other relevant stakeholders through Town Hall meetings and providing practical resources, including Frequently Asked Questions (FAQs), factsheets, and user guides for incident reporting.

2. **Phase 2: Compliance and Enforcement Approach (1 January 2026 onwards)** – As the reporting regime matures and regulated entities become acquainted with the mandatory reporting obligation, the Department will graduate to a more active regulatory focus. More advanced guidance resources will be disseminated incorporating feedback from Phase 1.

How long do I have to report a ransomware or cyber extortion payment that I have made?

As per section 27 of the *Cyber Security Act 2024*, you have **72 hours to make a ransomware or cyber extortion payment report** from the time when you make the ransomware or cyber extortion payment, or from the time you are aware a payment has been made on your behalf.

What do I need to report?

Subsection 27(2) of the *Cyber Security Act 2024* prescribes basic information that must be contained in a ransomware or cyber extortion report. **Section 7** of the Cyber Security (Ransomware Payment Reporting) Rules 2025 prescribes more specificity on what information needs to be contained within a ransomware payment or cyber extortion report. This information includes the following, where it is known or able to be known by reasonable search or enquiry:

- the contact and business details of the entity that made the payment, including an Australian Business Number (ABN);
- details of the cyber security incident, including its impact on the reporting business entity
    - 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
    - the impact of the incident on the reporting business entity's customers
    - what variant (if any) of ransomware or other malware was used
    - what vulnerabilities (if any) in the reporting business entity's systems were exploited; and
    - information that could assist the response to, mitigation or resolution of the cyber incident by a Commonwealth body, or State body – for example, this may include the Australian Signal's Directorate or the Australian Cyber Security Centre;

- the other entity's contact and business details including the ABN and address (in cases where the ransom was paid by another entity);
- the demand made by the extorting entity
    - the amount or quantum of the ransomware or cyber extortion payment (including non-monetary benefits) demanded and the method of provision demanded
- the ransomware payment;
    - the amount or quantum of the ransomware or cyber extortion payment (including non-monetary benefits) given and the method of provision
- communications with the extorting entity relating to the incident, demand and the payment
    - the nature and timing of any communications with the extorting entity
    - a brief description of those communications (if any)
    - a brief description of any pre-payment negotiations undertaken in relation to the ransomware demand or payment
- other information relating to the cyber security incident in the ransomware payment report.

Why does the Government need to collect ransomware payment reporting information?

The Department of Home Affairs and the Australian Signals Directorate will collect ransomware payment and cyber extortion reporting information as outlined in the *Cyber Security Act 2024* and the Rules for three key purposes:

- to allow the Government to observe what threat actors are most active, what types of entities and businesses they target, what types of code and malicious software (e.g. ransomware, malware, etc.) are used to extort entities, threat actors' preferred method of contact, and how much money or productivity is lost in the Australian economy
- to assist the Government in disseminating tailored advice to industry, particularly small and medium-sized enterprises (SMEs) on how to uplift their cyber hygiene, protect and secure their data, and make them **hard targets** for cyber criminals based on the trends identified in mandatory reports
- to assist the Government in future legislative proposals and other programs that directly target the scourge of ransomware and cyber extortion within the Australian economy.

Will ransomware information I provide to the Department be covered by the 'limited use' provision?

- Information that is provided to the Department under Part 3 of the *Cyber Security Act 2024*, but not to the National Cyber Security Coordinator (the Coordinator) will not be treated as 'limited use' information for the purposes of Part 4. There are information protection provisions under Part 3 of the *Cyber Security Act 2024* that apply to the information provided in a ransomware payment report, detailed below.

Can any information I provide be used against me in court or for regulatory action?

- Any information contained within a ransomware payment or cyber extortion report **is not admissible** for criminal proceedings, civil proceedings for contravention of a civil penalty provision, breaches of any Commonwealth, State and Territory law (including the common law) or for proceedings before a tribunal of the Commonwealth, any State or Territory (see **section 32**). Furthermore, this reporting obligation does not otherwise affect a claim of legal professional privilege (see **section 31**).
- There are some exclusions and exceptions. These include in criminal proceedings for the provision of false or misleading information or obstruction of Commonwealth public officials, in civil proceedings for a contravention of a civil penalty provision in the *Cyber Security Act 2024*, or in Royal Commissions or coronial inquiries, due to the significant sensitivity and gravity of those proceedings.

What can the Government do with information I provide in a ransomware payment report?

As outlined in section 29 and section 30 of the *Cyber Security Act 2024*, entities including the Department of Home Affairs and the Australian Signals Directorate may only use and disclose information contained in a mandatory ransomware payment and cyber extortion report for a permitted purpose, including:

Assisting the reporting business entity, and other entities acting on their behalf, to respond to, mitigate or resolve the cyber security incident.

Performing functions or exercising powers under Part 3 or Part 6 (as it applies to Part 3) of the *Cyber Security Act 2024*.

Proceedings under section 137.1 or 137.2 of the *Criminal Code* (false and misleading information and documents).

Proceedings under section 149.1 of the *Criminal Code* (obstruction of Commonwealth public officials).

Performance of the functions of a **Commonwealth body** or the **National Cyber Security Coordinator** relating to responding to, mitigating or resolving a cyber security incident.

Informing and advising the Minister of Cyber Security, and other Ministers of the Commonwealth about the cyber security incident.

The performance of the functions of an intelligence agency.

The Government **cannot use or disclose** information contained within ransomware payment or cyber extortion reports for any other purpose, that is not by a permitted purpose set out in sections 29 and 30 of the *Cyber Security Act 2024*.

What if I don't report within the prescribed 72-hour timeframe?

The *Cyber Security Act 2024* provides that a civil penalty of 60 penalty units may apply where a reporting business entity fails to make a mandatory ransomware payment or cyber extortion report. As detailed above, the Department is adopting an 'education-first' approach to regulation for the *Cyber Security Act 2024*, with a focus on assisting and supporting entities to meet their legal obligations in the first six months before the Department will transition to a more active regulatory focus.

Where can I go to get help and seek further information?

Please visit the Department's website page that details the legislation and provides some additional factsheets at: Cyber Security Act and the Cyber and Infrastructure Security Centre's website at: Town halls and awareness sessions for more information on the Town Hall sessions hosted in late 2024 and early 2025.

Email ransomware.reporting@homeaffairs.gov.au for any queries about your new ransomware and cyber extortion payment reporting obligation. This inbox is monitored Monday through to Friday, 9:00AM to 5:00PM.