



**SOCIAL
CYBER
INSTITUTE**

Strengthening Privacy Protection Against Contemporary Cyber Risk

Submission on the Exposure Draft of the *Privacy Amendment (Personal Data Protection) Bill 2026*

Submitted to the Australian Government Attorney-General's Department

18 September 2026

Prepared by

Mr Alfred Muscat

Associate Research Fellow | Social Cyber Institute

Approved for submission

Dr Greg Austin

Co-founder and Research Director of the Social Cyber Institute

This submission does not represent an agreed view of all researchers associated with the Social Cyber Institute.

Executive Summary:

The proposed reforms to Australia's privacy framework represent an important step towards strengthening the protection of personal information in an increasingly interconnected digital environment. However, several aspects of the proposed framework would benefit from further refinement, particularly where the speed and severity of contemporary cyber incidents can expose individuals and institutions to significant harm before conventional regulatory processes have begun.

Key Recommendations:

This submission recommends that the legislation should:

1. Adopt a graduated 24/48/72-hour breach reporting framework, with shorter notification periods applying where a breach involves highly sensitive information, poses a serious risk of harm, or may affect interconnected organisations or systems.
2. Clarify the obligation to mitigate harm following a data breach, including the considerations relevant to ransomware, cyber extortion and the payment or non-payment of ransom demands.
3. Recognise passwords, unique identifiers and authentication information as particularly sensitive data, given their capacity to facilitate identity theft, account compromise, credential stuffing and further cyber intrusion when combined with information obtained from other data breaches.

Policy Context:

Australia's privacy framework must reflect the realities of modern cyber incidents, whereby breaches are fast-moving, interconnected and cumulative. By the time an organisation detects a compromise, an attacker may already have accessed systems for days or weeks, extracted data, established persistence or begun exploiting credentials elsewhere. In that environment, delay increases risk. Reporting obligations should therefore enable early intervention, not simply record an incident after the fact.

1: Data breach reporting timeframes:

Recommendation: Amend s 26WK of the *Exposure Draft* so that the proposed 72 hours operates as an absolute maximum, not the ordinary reporting period. Further, a 24-hour preliminary notification requirement for serious, sensitive or interconnected breaches should also be introduced.

The proposed 72-hour timeframe should be considered alongside s 26WH of the *Privacy Act 1988* (Cth). Under s 26WH, an entity that reasonably suspects an eligible data breach must undertake a reasonable and expeditious assessment and take all reasonable steps to complete that assessment within 30 days. The proposed 72-hour reporting period under s 26WK begins only once the entity has reasonable grounds to believe that an eligible data breach has occurred.

Accordingly, 72 hours should not be viewed as notification within three days of the original compromise. A cyber incident may already have remained undetected for days or weeks, followed by a period of assessment under s 26WH, before the 72-hour clock begins.

The exposure draft also permits an incomplete initial statement where it is impossible or impracticable to provide all required information within the reporting period, with further information to be supplied as soon as practicable. This supports a staged reporting model: early notification need not require a completed forensic investigation.

Article 33 of The General Data Protection Regulation ('GDPR') provides a useful comparison. The GDPR requires notification "without undue delay and, where feasible, not later than 72 hours". The 72-hour period is therefore an outer limit, not a default waiting period.

Australia should adopt the same principle, while applying a stricter standard to higher-risk incidents.

A 24-hour preliminary notification should be required where:

- sensitive information is involved;
- malicious access appears ongoing;
- critical or interconnected systems are affected; or
- there are reasonable grounds to believe another entity may also be compromised.

This is particularly important because s 26WK(4) already contemplates breaches affecting multiple entities, but only provides that the reporting entity 'may' identify those other entities. Where another entity may be affected, earlier notification allows regulators and affected organisations to check systems, contain further compromise and reduce cascading harm.

The purpose of a 24-hour requirement is not to require certainty within 24 hours. It is to ensure that uncertainty does not justify silence.

As the Roman maxim warns, *dum Romae consulitur, Saguntum expugnatur* — while Rome deliberates, Saguntum falls. In cybersecurity, delay is itself a risk.

Proposed approach:

- 24 hours: preliminary notification for high-risk or interconnected incidents;
- 48 hours: supplementary information where available;
- 72 hours: fuller notification, with later updates where necessary.

At minimum, s 26WK should require notification "without undue delay and, in any event, within 72 hours."

2: Mitigation and ransomware:

Recommendation: Amend s 26WDB of the *Exposure Draft* to expressly provide that an entity's refusal to make a ransomware or cyber-extortion payment does not, of itself, constitute a failure to take reasonable steps to prevent or reduce harm.

s 26WDB requires an entity that reasonably believes or suspects a data breach has occurred to take, "as soon as practicable, reasonable steps to prevent or reduce harm" to affected individuals. The Bill also contemplates remedial action capable of reducing the likelihood of serious harm.

The obligation is appropriate, but its application to ransomware is unclear.

In a ransomware or cyber-extortion incident, an attacker may threaten to publish stolen personal information unless payment is made. This raises an important legal question: if payment could theoretically prevent publication of that information, could an organisation's refusal to pay later be characterised as a failure to take reasonable steps to reduce harm?

The legislation should answer that question expressly: no.

This is particularly important because the Australian Cyber Security Centre advises organisations not to pay cyber-extortion payments because payment provides no guarantee that information will be recovered or that stolen information will not subsequently be published or sold.

The *Cyber Security Act 2024* similarly regulates what occurs if certain entities make a ransomware payment by imposing a reporting obligation; it does not require or prohibit an entity to make one.

The privacy framework should therefore avoid creating a contrary incentive. An organisation should not face the argument that, by following government advice and refusing an extortion demand, it failed to mitigate harm under the Privacy Act.

The Bill should clarify that:

- refusing to pay a ransom does not, by itself, breach the duty in s 26WDB;
- ransom payment is not a prerequisite to establishing that reasonable mitigation steps were taken;
- the reasonableness of mitigation should instead be assessed by reference to measures within the organisation's control, including containment, securing compromised systems, protecting affected individuals, notifying relevant authorities and reducing further unauthorised access or disclosure; and
- conversely, payment of a ransom should not automatically establish that harm has been mitigated, particularly where there is no reliable assurance that stolen information has been deleted.

The purpose of s 26WDB should be to require organisations to respond reasonably to a breach — not to place them under an implied legal obligation to fund the person responsible for it.

A simple statutory clarification would remove that uncertainty:

For the avoidance of doubt, an entity does not fail to comply with this section merely because the entity does not make a payment or provide another benefit in response to a ransomware or cyber-extortion demand.

This would preserve the duty to mitigate harm while ensuring that the Privacy Act cannot inadvertently be interpreted as requiring, or encouraging, ransom payments.

There is also a broader policy risk in leaving the position unclear. If ransom payment comes to be viewed as a component of legally adequate mitigation, this may encourage greater reliance on cyber-insurance products that cover extortion payments and embed payment as an expected incident-response cost.

That, in turn, risks creating a moral hazard. The more predictable and insurable ransom payments become, the more attractive insured organisations may appear to cybercriminals, reinforcing the economic incentives that sustain ransomware attacks. The legislation should therefore avoid creating any implication that payment is an expected or preferred form of mitigation.

3: Passwords and security question responses:

Recommendation: Amend s 6FD of the *Exposure Draft* so it explicitly recognises unique passwords, passphrases and security question responses as examples of personal information or identifiers capable of contributing to an individual being reasonably identifiable.

Proposed s 6FD defines personal information as information or an opinion relating to an identified or reasonably identifiable individual. Its examples include names, dates of birth, addresses, contact information, pseudonyms, identifiers and location data. However, the exposure draft does not expressly mention passwords or security question responses. That omission does not reflect the practical value of authentication credentials in modern data breaches.

A password is not merely a mechanism for accessing one account. Where a person reuses the same or similar password across multiple services, a compromised credential can connect otherwise separate accounts and datasets. A password disclosed in one breach may be associated with an email address in another, a username in another and identifying information elsewhere. In combination, those fragments can assist in linking accounts to the same individual, accessing further personal information and constructing a considerably more complete picture of that person's identity.

Security question responses present a similar, and potentially greater, concern. Answers such as a mother's maiden name, first school, childhood street or pet's name may themselves reveal personal information and may be reused as authentication information across different services.

This approach would be consistent with other Commonwealth legislation. The *Crimes Act 1914* (Cth), for example, s 3ZZUK expressly defines “account credentials” to include a username, password, PIN and a security question or answer.

The amendment need not substantially expand the existing concept of personal information. Rather, it would clarify how that concept applies to contemporary digital identity. Proposed s 6FD already recognises that an individual may be identifiable without their legal name and expressly includes pseudonyms and identifiers. Authentication credentials are a logical extension of that principle.

It is difficult to justify a modern privacy framework that expressly recognises geolocation, behavioural patterns and pseudonymous identifiers, but does not expressly recognise one of the most consequential forms of information exposed in a cyber breach: the credentials capable of unlocking, connecting and identifying an individual's digital accounts.

Overall Position:

The Exposure Draft is a significant opportunity to modernise Australia's privacy framework, but effective reform must reflect the practical realities of contemporary cyber incidents. Speed, certainty and the nature of compromised information matter.

The amendments proposed in this submission are relatively targeted. They do not seek to impose unrealistic obligations on organisations or require that a cyber incident be fully understood before action is taken. Rather, they seek to ensure that the law encourages early notification where delay may increase harm, provides certainty as to what reasonable mitigation requires, and recognises that authentication credentials such as passwords and security question responses can be among the most consequential information compromised in a data breach.

A modern privacy regime should not merely regulate what happens after personal information has been compromised. It should be designed to reduce the capacity of an initial breach to develop into further harm. The proposed amendments would assist in ensuring that Australia's privacy framework is responsive not only to the existence of a data breach, but also to the speed, interconnectedness and cumulative nature of digital harm.