WHO? Government Agency / Regulator to be notified	**WHO?** Scope of application	**WHAT?** Trigger for notification obligation	**WHEN?** Max timeframe for notice to be given	**HOW?** Method for notification	**WHY?** Act or regulation	**WHY?** Penalty for non-compliance
Office of the Australian Information Commissioner (OAIC)	APP Entities – including agencies or organisations with an annual turnover of more than $3 million, and other organisations covered by the *Privacy Act 1988* (Cth) (see guidance **here**)	Eligible Data Breach – where unauthorised access, disclosure or loss of personal information is likely to result in serious harm	As soon as practicable after forming reasonable grounds to believe an eligible data breach has occurred (entities must take reasonable steps to complete an assessment within 30 days of first suspecting an eligible data breach may have occurred)	Notification statement to the OAIC, and notification statement to impacted individuals meeting criteria in Privacy Act 1988 (Cth)	*Privacy Act 1988* (Cth)	Up to a maximum of • $50M; or • 3x benefit derived; or • 30% turnover during period of breach *(Corporations)* See also: right of individuals to seek a remedy under tort for '**serious invasions of privacy**' in certain circumstances (see guidance **here**).
Australian Cyber Security Centre (ACSC)	Reporting Business Entities – includes any organisation with an annual turnover of more than $3 million	In the event of a payment of a ransomware or cyber extortion payment.	Within **72 hours** of making the payment	**Online Form** (cyber.gov.au)	*Cyber Security Act 2024* (Cth)	For a failure to notify the ACSC of a ransom payment made: **$19,800** *(Individuals)* **$99,000** *(Corporations)*
	Owners/operators of 'critical infrastructure assets' (see guidance **here**)	"Critical" cybersecurity incident (i.e., when there is a *significant* impact on the availability of the asset)	Critical Incidents **Within 12 hours** (If initial report is oral, written report must be lodged within 84 hours)	Orally: **1300CYBER1** (1300292371) Written: **Online Form** (ReportCyber)	*Security of Critical Infrastructure Act 2018* (Cth)	Up to **$33,000**, comprising: Failure to notify or notify in time: **$16,500** AND/OR Failure to use approved form / failure to follow up verbal report in writing: **$16,500**
		Other cybersecurity incident (i.e., when there is a *relevant* impact on the availability, integrity, reliability, or confidentiality of the asset)	Other incidents: **Within 72 hours** (If initial report is oral, written report must be lodged within 48 hours)			

	Holders of a carrier licence pursuant to the *Telecommunications Act 1997* (Cth)	As above	As above	As above	As above	As above for SOCI Act reporting
	Carrier Service Providers (CSPs) providing telecommunication services on network units owned by other entities as defined by the *Telecommunications Act 1997*				As above	As above for SOCI Act reporting
	An accredited data recipient in a designated sector (currently Banking, Energy)	Security incident	As soon as practicable, and no later than **30 days**	As above	*Competition and Consumer (Consumer Data Right) Rules 2020* (Cth)	As a result of failure to protect data (not necessarily a failure to notify): **Greater of:** • $10 million; • 3 x total value of benefits obtained from the breach; and • 10% of annual domestic turnover
Australian Prudential Regulation Authority (APRA)	APRA-regulated entities (banks, authorised deposit taking institutions (ADI), superannuation funds (RSE Licensees), insurance companies)	Information security incident (with material effect on the entity or the interests of depositors, policyholders, beneficiaries, or other customers, or which has been notified to other regulators)	**72 hours** (but as soon as possible)	To a regulated entity's usual APRA contacts, or: **APRA Extranet** (Online Form) Or applicable form by email or post.	CPS 234 Information Security *Superannuation Industry (Supervision) Act 1993* *Life Insurance Act 1995* *Insurance Act 1973* *Banking Act 1959* *Private Health Insurance (Prudential Supervision) Act 2015*	Failing to notify APRA of a breach of CPS 234 is an offence, with differing fixed penalties per industry: **$66,000** *(Banks)* **$9,900** *(Private Health Insurers)* **$16,500** *(RSE Licensees)* **$66,000** *(ADIs, Life Insurers, General Insurers)*

Australian Securities & Investments Commission (ASIC)	Australian Financial Services and credit licensees	'Reportable situation' – Note that this could include a significant breach or likely significant breach of 'core obligations' including investigations into significant breaches	Within **30 days**	Via the approved form on the entity's ASIC Regulatory Portal	RG 78 – Breach reporting by AFS Licensees and Credit Licensees *Corporations Act 2001* (Cth)	**Civil Penalties:** For Individuals- for example, sole practitioners with AFSLs, greater of: • $1.7M; and • 3 x total value of benefits obtained from the breach. For corporations, greater of: • $16.5M; • 3 x total value of benefits obtained from the breach; and • 10% of annual domestic turnover Criminal Penalties: • **$79,200**; (Individuals) • **$792,000**; (Corporations) and/or • 2 years imprisonment
Australian Securities Exchange (ASX)	ASX-listed entities	Where information that is likely to have an effect on the value of the entity's securities is held (including cybersecurity incidents that are of such size and scale that it requires immediate disclosure)	Immediately (and a trading halt needs to be considered if a full disclosure cannot be made immediately)	To an ASX-listed entity's usual listings adviser, via ASX Online	*Corporations Act 2001* (Cth) ASX Listing Rules	Suspension in trading of the entity's securities. In an extreme case, removal of the entity from the ASX list.

Australian Digital Health Agency (ADHA)	Healthcare providers using the My Health Record System	Data Breach (including any event/circumstance that will/may compromise the security or integrity of the system - e.g., ransomware incident)	As soon as practicable after becoming aware of the breach/security incident	Statement to the ADHA and individual notifications **AND** Statement to the OAIC and individual notification	*My Health Records Act 2012* (Cth) *Privacy Act 1988* (Cth)	**ADHA:** **$495,000** **OAIC:** Greater of: • $50M; or • 3x benefit derived; or • 30% turnover during period of breach. *(Corporations)*
Australian Transaction Reports and Analysis Centre (AUSTRAC)	Reporting entities governed by AUSTRAC (Financial Services, Bullion Traders, Gambling Services)	Payments suspected to be related to the financing of criminal activity	**24 hours** (If related to terrorism financing) **3 days** (Other criminal activity)	**Online 'Suspicious Matter Report' Form** (AUSTRAC Online)	*Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth)	For failure to meet AML/CTF obligations, civil penalty orders can be made by the Federal Court for up to: **$6.6M** *(Individuals)* **$33M** *(Corporations)*