D. Other legislative requirements

Cyber incident reporting and response obligations

Public sector entities, including local governments, deliver a broad range of services. In Chapter 3, we refer to the specific 'core' Queensland legislative and policy requirements for these entities. In addition to these, due to the nature of the services some Queensland public sector entities provide, they must also comply with 'other' state and commonwealth requirements. Figure D1 shows the other key legislative obligations specific to cyber incident response for Queensland public sector entities, as reported by the Cyber and Infrastructure Security Centre, within the Department of Home Affairs (Commonwealth).

Figure D1
Other legislative requirements for cyber incidence response

Requirement and Act	Description	Applicable to
Personal information data breach obligations *Privacy Act 1988* (CWTH) and *Information Privacy Act 2009* (QLD)	Requirement to notify affected individuals, the Office of the Australian Information Commissioner (OAIC), and Office of the Information Commissioner Queensland (OIC) when a data breach is likely to result in serious harm to an individual whose personal information is involved. Requirement to conduct a reasonable and expeditious assessment of a suspected eligible data breach, taking all reasonable steps to ensure that this assessment is completed within 30 days.	May apply to any public sector entity that meets thresholds under the legislation.
Obligation to report cyber security incidents *Security of Critical Infrastructure Act 2018* (CWTH)	Obligation for an entity holding or operating critical infrastructure (services that are essential for everyday life, such as energy, communications, water, transport, and health, as defined by the *Security of Critical Infrastructure Act 2018*) to report a cyber security incident to the Australian Signals Directorate.	Applicable to those entities holding critical infrastructure as defined under the legislation. May include departments, statutory bodies, government owned corporations, or local governments.
Obligation to undertake a vulnerability assessment *Security of Critical Infrastructure Act 2018* (CWTH)	The Secretary of the Department of Home Affairs may give a notice requiring an entity holding a System of National Significance* (SoNS) to undertake a vulnerability assessment within a specified period.	Any entity holding critical infrastructure declared a System of National Significance (SoNS) as directed by the Minster for Home Affairs. May include departments statutory bodies, government owned corporations, or local governments.
Obligation to provide systems information *Security of Critical Infrastructure Act 2018* (CWTH)	The Secretary of the Department of Home Affairs may give a notice requiring an entity holding a SoNS to provide systems information. This notice can be in relation to periodic reporting of system information or in response to a specific event.	
Obligation to have incident response plans *Security of Critical Infrastructure Act 2018* (CWTH)	Obligation for entities holding a SoNS to have a written cyber security incident response plan detailing how the entity will respond to cyber security incidents that affect its systems.	

Requirement and Act	Description	Applicable to
Obligation to test an incident response plan *Security of Critical Infrastructure Act 2018* (CWTH)	Obligation for entities holding a SoNS to test preparedness, mitigation, and response capabilities to reveal whether existing resources, processes, and capabilities of an entity sufficiently safeguard being impacted by a cyber security incident.	Any entity holding critical infrastructure declared a System of National Significance (SoNS) as directed by the Minster for Home Affairs. May include statutory bodies, government owned corporations, or local governments.
Obligation to report to Australian Securities and Investments Commission (ASIC) *Corporations Act 2001* (CWTH)	Obligation to submit notifications about 'reportable situations' (which may include among other matters significant data breaches) to ASIC within 30 calendar days via the ASIC Regulatory Portal.	Government owned corporations who operate an Australian financial services licence.
Obligation to report to the Australian Digital Health Agency *My Health Records Act 2012* (CWTH)	Obligation to notify the Australian Digital Health Agency of any potential or actual data breaches that relate to the *My Health Record* system.	Any entity holding healthcare-related data which relates to the *My Health Record* system. May include departments or statutory bodies.

Note: * Systems of National Significance are a subset of critical infrastructure assets. They are considered to be of the highest criticality by virtue of their interdependencies across sectors and potential impact to other critical infrastructure assets and sectors if disrupted.

Source: Queensland Audit Office based on Cyber Security Obligations for Corporate Leaders by the Cyber and Infrastructure Security Centre.