

Critical infrastructure and security — the SOCI lens

Why data centres are regulated as critical infrastructure and what that obliges

The key idea: digital infrastructure is on the critical list

Australia's Security of Critical Infrastructure (SOCI) Act treats **data storage and processing** as a critical infrastructure sector, alongside energy, water, ports and hospitals. That single fact reframes the data centre near you: it isn't just a private building; it's part of a regulated national system with legal obligations to be resilient and secure.

What the SOCI framework requires

Operators of critical data storage and processing assets must register them, maintain a **risk management program** covering cyber, physical, personnel and supply-chain hazards and **report serious cyber incidents** to government within tight timeframes. For the most important systems, government holds step-in powers as a last resort in a serious attack. The Cyber and Infrastructure Security Centre (CISC) administers the regime; the Australian Cyber Security Centre (ACSC) provides the technical backbone.

The defence-adjacent question

Some facilities will host government, defence-related or otherwise sensitive workloads, raising the stakes for security clearances, ownership scrutiny and foreign-investment review. That's real and it doesn't make every data centre a defence asset. Most facilities host ordinary commercial services. The point of the framework is proportionality: obligations scale with what a facility actually holds and how critical it is.

What it means for communities

Security regulation mostly works invisibly, but it surfaces locally in legitimate ways: physical security design (fencing, setbacks, cameras) that shapes what neighbours see; reluctance to publicise some operational details; and emergency planning that should mesh with local services. Security is a reason for *care* in what's disclosed. It is not a reason to answer no planning questions. The two get conflated; communities shouldn't accept that.

What good practice looks like

- Proponents state plainly whether a facility is (or expects to be) a regulated critical asset.
- Security design explained at the level neighbours experience, without demanding operational secrets.
- Emergency and incident planning coordinated with local fire, police and council services.
- "Security" never used as a blanket refusal to engage with planning processes.

Questions to ask

Is this facility regulated under the SOCI framework? How does its emergency planning connect with our local services? Which questions can't be answered for security reasons and who has verified that the rest are answered?

Want to know more? The Cyber and Infrastructure Security Centre (cisc.gov.au) explains the SOCI regime; the ACSC publishes public security guidance. This sheet is general information, not legal advice; check the named sources for current detail.