

Government focus on critical infrastructure security and resilience

The Australian Government's *2020 Cyber Security Strategy*, released in August last year, flagged the introduction of an enhanced regulatory framework to drive an uplift in the security and resilience of Australia's critical infrastructure and systems of national significance.

In December 2020 the Department of Home Affairs introduced into Parliament the *Security Legislation Amendment (Critical Infrastructure) Bill 2020*, outlining the key elements of the proposed regulatory framework. The bill proposed a range of obligations for critical infrastructure operators, principally:

- A requirement for entities to have a Board approved critical infrastructure risk management program that follows sector-specific rules that address cyber security, physical security, personnel security, supply chain security and natural hazard risks (part of proposed *positive security obligations*).
- Mandatory reporting requirements for cyber security incidents.
- Enhanced cyber security obligations for the *most critical* of critical infrastructure entities (referred to as *systems of national significance*), including a requirement to conduct regular cyber security exercises and cyber vulnerability assessments.
- A requirement for critical infrastructure entities to cooperate with government during major cyber security events and, at times, follow directions issued by government to take specific actions (in relation to cyber security), or facilitate an intervention by a government agency. The focus of this obligation is on events that are too sophisticated or too disruptive for entities to manage alone.

PJCIS review and development of rules

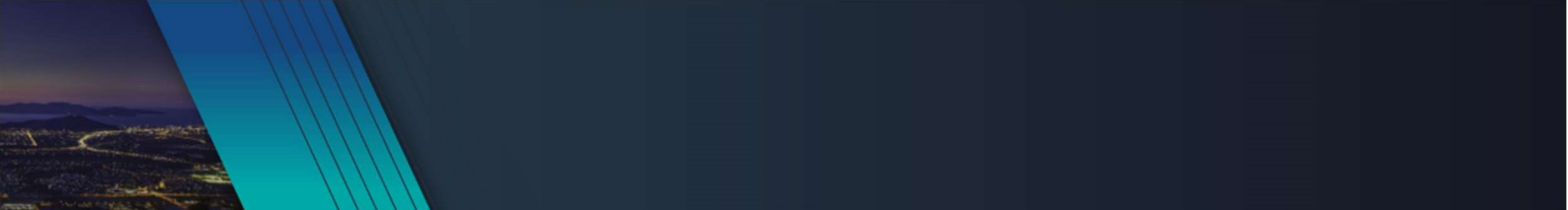
The bill was referred to the Parliamentary Joint Committee on Intelligence and Security (PJCIS) in December 2020 for review. This review process was expected to take around five months and the Department of Home Affairs expected the legislation to be in force from July 2021.

In April 2021 the Department of Home Affairs commenced co-development with the electricity sector on sector-specific rules (while the bill was still under review by the PJCIS). The electricity sector was the first industry to undergo this co-development process, with rules co-development with other sectors starting in a staggered manner over subsequent months.

This co-development process resulted in draft rules for each of the areas identified in the legislation:

- Cyber security – a requirement to achieve increasing levels of cyber security maturity, as defined under the Australian Energy Sector Cyber Security Framework (AESCSF)¹, within specific timeframes.
- Personnel security – a requirement to implement at-hire and periodic security vetting of critical employees, including using the government's AusCheck background checking process.
- Supply chain hazards – a requirement to implement a supply chain risk management program aligned with ISO 28000, ISO 28001 and ISO 22301, with a focus on managing supply chain risks arising from threats such as unauthorised access, misuse of privileged access and high risk vendors.
- Physical security hazards – a requirement to implement defence in-depth security at critical sites and conduct regular tests of these security measures to ensure their effectiveness and suitability.
- Natural hazards – a requirement to demonstrate a risk management program that addresses risks posed by events such as bushfires, floods, cyclones, storms, heatwaves, earthquakes, tsunamis and pandemics.

¹ Further information on the AESCSF is available on AEMO's [website](#).



These draft rules for the electricity sector were developed from April through to July 2021. For reasons unknown, the Department of Home Affairs paused co-development of the electricity sector rules in August 2021. Other sectors that had commenced after the electricity sector (such as the gas, water and data processing sectors) had their co-development programs slowed during August as well, and most co-development had stopped by late September. At the present time, all rules in all sectors remain in a draft state.

In late September 2021 the PJCIS delivered its final report. The PJCIS recommended the Department of Home Affairs revisit the development of the rules with each sector, reflecting on feedback that the bill should not progress until all industry sector rules had been finalised. The PJCIS also recommended the bill be split in two, with the risk management program elements of the bill (which reference the rules) to be deferred but all other aspects of the bill to be progressed as soon as practical.

Customer Panel discussion

As a transmission network service provider, Powerlink will be covered by all of the requirements in the bills.

The rules under the risk management program obligation will have the highest impact on Powerlink. The other requirements – such as mandatory reporting, conducting cyber security exercises or facilitating government directions in significant cyber security events – are not materially significant and in many ways reflect expected practice.

At our meeting, we would like to explore how these proposed regulations may impact on Powerlink (acknowledging the rules are still in draft and subject to change). Powerlink and other electricity sector entities may need to undertake additional significant investment, resourcing and risk management activities to achieve and maintain compliance with the rules (through the legislation). We are also interested in the Customer Panel's views on their interpretation of the rules and the government's objectives.