



Australian Government
Department of Home Affairs

Erin Cini
Director, Regulation and Compliance
Independent Pricing and Regulatory Tribunal
By Email

Dear Erin

Thank you for the opportunity to provide a submission to the 2019 Review of the Sydney Water Operating Licence. In particular I would like to thank IPART for specifically calling out the importance of critical infrastructure issues via Question 22 of the preliminary questions.

The Critical Infrastructure Centre (the Centre) was established in January 2017 to safeguard Australia from the increasingly complex national security risks of sabotage, espionage and coercion to our critical infrastructure. Rapid technological changes have resulted in critical infrastructure assets with increased cyber connectivity, and greater participation in, and reliance on, global supply chains with many services being outsourced and offshored.

While recognising that foreign involvement brings many benefits, it also exposes Australia's critical infrastructure assets to national security risks. Foreign involvement, through ownership, offshoring, outsourcing and supply chain arrangements, can increase a malicious actor's ability to disrupt critical infrastructure assets which could have a range of implications for business, government and the community.

As you are aware, to assist in managing these risks, the Government recently passed the *Security of Critical Infrastructure Act* (the Act). The Act strengthens the Australian Government's capacity to manage the national security risks resulting from foreign involvement in Australia's critical infrastructure. The Act contains three key measures to manage national security risks related to critical infrastructure: a Register of Critical Infrastructure Assets (the Register), an information gathering power, and a Ministerial directions power.

The Act only applies to specific assets in the electricity, gas, water and ports sectors which are characterised in part by the absence of regulatory regimes specifically designed to manage national security risks. Given this concern, the Centre encourages IPART to consider changes to the Sydney Water licence that specifically mitigate against national security risks.

While national security risks typically involve different threat actors to other business risks, in the Centre's experience, the protections that a critical infrastructure operator might put in place to manage those risks are often similar to those that apply to other risks.

As a starting point for the types of protections the Centre recommends be considered for inclusion in the Sydney Water licence, I would direct your attention to the recently amended licences for the NSW electricity networks TransGrid, Ausgrid and Endeavour which now all include critical infrastructure provisions relating to remote offshore access to operational technology along with provisions about data protection and storage.

The Critical Infrastructure Security Division is happy to provide more specific advice during the development of the draft licence to tailor a package of conditions that is appropriate for Sydney Water specifically.

Again I would like to thank you for the opportunity to comment on the Issues Paper and I look forward to further engagement during the review. The contact officer within the Division is Mr Lachlan Bickley [REDACTED]. Mr Bickley will be happy to assist with any questions

Yours sincerely

[REDACTED]
Pablo Carpay
First Assistant Secretary
Critical Infrastructure Security Division
Department of Home Affairs
23 August 2018