Australian Government
Critical Infrastructure Centre

Submission to the Review of Hunter Water's Operating Licence 2012-2017

This submission

The Critical Infrastructure Centre welcomes the opportunity to make this submission to the Review of Hunter Water's Operating Licence 2012-2017.

This submission provides an unclassified outline of:

- the national security risks associated with critical infrastructure, including in the water sector, and
- potential mitigations that could be considered to manage national security risks.

Further detail can be provided to IPART on request.

The importance of the water sector and Hunter Water Corporation

A clean and reliable supply of water is essential to all Australians, and many of our other critical infrastructure sectors and businesses. A disruption to Australia's water supply or water treatment facilities could have major consequences for the health of citizens and impact the diverse range of businesses that rely on water — from the cooling towers used at power stations, to food processing.

Hunter Water Corporation (Hunter Water) provides water and wastewater services to six local government areas in New South Wales, including the Lower Hunter region north of Sydney. The service area supports a population of over 550,000 people in an area of over 6,000 square kilometres. The region includes Newcastle, Cessnock, Maitland and Lake Macquarie. The economic value of the Hunter Water footprint is $30.8 billion, 6.5 per cent of NSWs economic output. This includes $3.2b (nearly 10 per cent) of NSW's manufacturing.

Within the Hunter region, a number of critical infrastructure assets depend on the ongoing integrity of Hunter Water assets. These include:

- *Wate*r - there is an interconnection (both ways) between Hunter Water and the water system operated by Wyong and Gosford City Councils.
- *Electricity Generation* - the Eraring scheduled generator sits within in Hunter Water's service area, and the generators of Vales Point B and Colongra are just outside of the Hunter Water service area and may have some dependence on the interconnection when it is in use.
- *Defence* - RAAF Base Williamtown.
- *Ports* - Newcastle Port handles 14 per cent of Australia's bulk cargo and is within Hunter Water's service area.

National security risks to critical infrastructure, including the water sector

The national security risks to critical infrastructure are complex and have continued to evolve over recent years. In addition, critical infrastructure assets are subject to rapid technological change with increased cyber connectivity, and increasingly engaged in global supply chains with services being outsourced and offshored. While owners and operators understand and manage many of the risks to the continuity of their operations as a core part of their business, the Australian Government is seeking to ensure they have a more detailed understanding of the national security risks of sabotage, espionage and coercion.

Australia's water assets are potentially vulnerable to sabotage, espionage and coercion.

In relation to **espionage**, water companies hold detailed customer usage data. Such holdings of data represent attractive targets for foreign intelligence services to target particular individuals or gain insights into particular customers and their activities (e.g. Defence operations), or inform sabotage of other critical infrastructure sectors.

In relation to **sabotage**, a hostile actor could take advantage of operational access through outsourcing, offshoring and supply chain arrangements to disrupt water supply, damage other critical infrastructure assets, and erode public trust in government services.

In recent years, there has been a trend to outsource, including through greater outsourcing of maintenance services, design and construction work. The *Australian Infrastructure Plan: Priorities and reforms for our nation's future* (2016) notes that privatisation of water assets is expected in the next five years.

Potential Mitigations

A range of licence conditions could be considered to minimise the potential for malicious actors to access and control Hunter Water, including requiring:

- key personnel to hold security clearances,
- information about operational technology (such as SCADA systems) and associated ICT infrastructure be held solely within Australia,
- appropriate security controls implemented to prevent the export of personal data records, and
- limitations on remote access to operational systems.

Critical Infrastructure Centre

On the 23rd of January 2017, the Australian Government launched the Critical Infrastructure Centre (the Centre) in response to the complex and evolving national security risks to critical infrastructure.

The Centre will work across all levels of government and with critical infrastructure owners and operators to identify and manage national security risks to our most critical assets in the face of espionage, sabotage and coercion – risks we are exposed to now more than ever. It forms part of the Government's broader strategy to build the resilience of our critical infrastructure in the face of all hazards. The Centre understands that state, territory and industry mechanisms already exist which may assist in managing national security risks, and will work closely to leverage such mechanisms where possible.

The Critical Infrastructure Centre would be happy to work with IPART and Hunter Water to provide more detailed classified advice to ensure that the Hunter Water licencing regime codifies key national security requirements as operating conditions.

The Critical Infrastructure Centre can be contacted on (02) 6141 3338 or cicentre@ag.gov.au.