Australian Government
Critical Infrastructure Centre

Submission to the Review of the WaterNSW Operating Licences

This submission

The Critical Infrastructure Centre (the Centre) welcomes the opportunity to make this submission to the Review of the WaterNSW operating licences.

This submission provides an unclassified outline of

- the national security risks associated with critical infrastructure, including in the water sector, and
- suggests provisions for the operating licence which could enable better management of those risks.

Further detail can be provided to IPART on request.

The importance of the water sector and WaterNSW

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.

WaterNSW is Australia's largest water supplier and New South Wales' major supplier of raw water. The primary use of water supplied by WaterNSW is agricultural.

Power stations that use water from dams managed by WaterNSW include: Mount Piper, Liddell, Bayswater, Blowering, Hume and Shoalhaven. Together, these power stations account for approximately 43 per cent of NSW scheduled installed capacity.

National security threats to critical infrastructure, including the water sector

The national security risks to critical infrastructure are complex and have continued to evolve over recent years with advances in technology, increased cyber connectivity and engagement in global supply chains. Recent trends to outsource maintenance services and design and construction work, as well as a greater degree of foreign investment, increase the potential vulnerability of Australia's water assets to targeted or opportunistic hostile foreign intelligence activity. Sensitive information, including personal customer details, could be compromised. Managers could be coerced into decisions that favour a foreign state. Intellectual property or valuable commercial information could be stolen. Malicious foreign actors will often obscure their activities and intentions behind legitimate business deals or corporate activity, and individuals may be knowingly or unknowingly manipulated to fulfil the role of trusted insider. Such operations may take years to come to fruition. Recognition of national security threats must form part of any risk assessment for industries providing or linked to Australian critical infrastructure. Such assessments should also consider appropriate mitigation efforts designed to eliminate, limit or manage the threats to national security.

Management of risks

In order to allow WaterNSW and the Centre to work together to manage the national security risks to WaterNSW's critical infrastructure, the Centre suggests that IPART consider the inclusion of provisions within the WaterNSW operating licence which require WaterNSW to:

- Collaborate with the Critical Infrastructure Centre to ensure the management of national security risks.
- Ensure key operational personnel hold a Negative Vetting Level 1 security clearance.

Under this approach, the Centre and WaterNSW could work together as active partners to tailor mitigations to national security risks that are specific and relevant to WaterNSW. The Centre could work with WaterNSW to enhance its understanding of national security risks to its critical infrastructure, and the Centre would benefit from WaterNSW's expert knowledge of the infrastructure itself.

As part of the collaboration, a range of key measures could be considered to minimise the potential for malicious actors to access and control WaterNSW. These may include:

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

Key personnel to hold security clearances

The Centre recognises that in most cases, neither industry nor government in isolation has all the information they need to understand and mitigate risks.

A requirement for key personnel in WaterNSW, such as senior operational managers, to hold security clearances, would facilitate the exchange of classified security information between the Centre and WaterNSW to ensure a better understanding of the national security risks to critical infrastructure.

Locating operational technology and associated ICT infrastructure solely in Australia

Locating operational technology and associated ICT infrastructure offshore increases the number of vectors of risk to critical infrastructure. Malicious actors would have greater ability to access Australian critical infrastructure overseas, and conversely, governments, owners and operators of critical infrastructure would

have less visibility of possible unauthorised access. Moreover, governments may not have jurisdiction to monitor or prosecute malicious action committed overseas.

Implement security controls to prevent export of personal data records

As discussed above, water services possess significant data holdings about customers, which are attractive targets for malicious actors. Customer data may assist malicious actors to gain an insight into customers' activities, or inform sabotage of other critical infrastructure sectors. This risk may be mitigated by implementing conditions to prevent the export of personal data records overseas.

Limit remote access to operational systems

Remote access to operational systems creates vectors through which malicious actors can access and control the operation and continuity of water services.

Carefully considering and managing remote access to operational systems can assist to minimize the number of vectors through which malicious actors can influence the operation of water infrastructure.

Critical Infrastructure Centre

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

The Centre works 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.

As outlined above, the Centre would be happy to work collaboratively with IPART and WaterNSW to ensure appropriate management of national security risks.

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