Speech By

# Patrick Weir

## MEMBER FOR CONDAMINE

Record of Proceedings, 18 October 2018

## STATE DEVELOPMENT, NATURAL RESOURCES AND AGRICULTURAL INDUSTRY DEVELOPMENT COMMITTEE

### Report, Motion to Take Note

**Mr WEIR** (Condamine—LNP) (3.31 pm): I rise as a member of the State Development, Natural Resources and Agricultural Development Committee to speak to Auditor-General's report No. 19 titled *Security of critical water infrastructure*. On 8 August 2017 Auditor-General report No. 19 titled *Security of critical water infrastructure* was referred to the Public Works and Utilities Committee of the 55th Parliament. That committee did not report before the dissolution of parliament on 29 October. The report was referred to the State Development, Natural Resources and Agricultural Industry Development Committee on 3 May 2018.

In Queensland, water service providers monitor and control water transport, treatment and distribution. This includes the water distribution network for drinking water, reservoirs and pump stations and collection and treatment of wastewater. Water control systems in Queensland have been maliciously targeted, resulting in danger to public health and safety. The Queensland Audit Office identified that attacks have resulted in overflows of untreated sewage, reductions in water pressure or shutdowns in the distribution of water. As many of these systems are now connected to other networks and the internet, the risk of unauthorised access has increased.

The audit was conducted because of the necessity for secure critical infrastructure, heightened security risks and cyber attacks leading up to the Commonwealth Games and a previous audit of systems used to manage traffic signals that found control systems were not secure and susceptible to targeted attacks. The Auditor-General told the committee—

Targeted attacks previously have resulted in overflows of untreated sewage and shutdowns in the distribution of water. We acknowledge that entities cannot always prevent attacks through information technology, but they can strengthen their defences. They also need to implement processes to detect and recover from security breaches, enhancing cyber resilience.

All entities audited were found to be susceptible to security breaches or hacking attacks because of weaknesses in processes and controls. The entities reported that they could operate smaller plants or parts of their larger water treatment plants manually in the event of disruption to computer systems, but had not demonstrated this capacity. Only one entity had documented its manual operating procedures and none had ever tested running their whole plants manually.

The audit report made a number of recommendations, which we just heard about from the chair of the committee. They included: integrating information technology; facilitating information sharing; and improving oversight. It recommended simple things like implementing KPIs. We have asked for an update on this. This was a disturbing report. Security was so lax on such critical pieces of infrastructure. I thank the other members of the committee for their work. I look forward to a better audit report on water security the next time around.