Speech By

Jessica Pugh

MEMBER FOR MOUNT OMMANEY

Record of Proceedings, 18 October 2018

STATE DEVELOPMENT, NATURAL RESOURCES AND AGRICULTURAL INDUSTRY DEVELOPMENT COMMITTEE

Report, Motion to Take Note

Ms PUGH (Mount Ommaney—ALP) (3.43 pm): I rise to speak on the committee report on water cybersecurity and the QAO audit of critical infrastructure. As we have heard, the Department of Natural Resources, Mines and Energy have worked closely with the Queensland Audit Office throughout the audit. It should be noted that they are committed to implementing the two relevant QAO recommendations. These recommendations were to integrate information technology risks and cyberthreats into the existing risk management framework for drinking water services and in the Queensland water and sewerage service provider performance reports and also to facilitate information sharing about adopting standards for securing information technology amongst entities that manage water control systems.

The department regulates drinking water quality and service provider performance. The department is committing to adapt the regulatory framework to ensure cybersecurity and information technology hazards are assessed by water and sewerage service providers and that these outcomes are reported. These adaptions will be developed in consultation with the relevant service providers and industry bodies to ensure that they are both relevant and cost-effective. A project is underway to collect data that will inform this process.

There are 84 registered providers of drinking water services operating over 300 drinking water supply schemes across Queensland, with 45 per cent of service providers having fewer than 1,000 connections—which means that they are servicing relatively small amounts. The QAO report is based on audits of three drinking water service providers, all of which are very large urban providers. These providers are more likely to be vulnerable to security related issues that have technological components to their systems. The entities audited have already begun implementing improvements in their management of cybersecurity, and this was acknowledged in the report.

The use of technology varies greatly across providers and hence the susceptibility to information technology and cybersecurity issues. For example, there are many providers that do not have supervisory control and data acquisition, or SCADA, systems or that do not have SCADA systems that are integrated into a broader network. A number of good practice guidance documents already exist that can and are being used by the relevant providers to establish or improve their resilience against cyber and information technology risks.

The department has engaged a contractor to undertake investigations with six medium to large service providers as a pilot to determine the extent and type of potential of cybersecurity threats. This study will provide data to help the government determine what needs to be incorporated into the existing framework and how best to implement it. We as a government are working with water industry bodies and keeping service providers informed about the project.

I would like to finish by thanking my committee mates. It has certainly been a very diverse and interesting year for our committee and it is not over yet. I have enjoyed it so far. We have looked at everything from fisheries to farm yards. It has been lots of fun—long may it continue.