Parliamentary Committees

Consideration of the Auditor-General's Report 19: 2016-17

Security of critical water infrastructure

Report No. 11, 56th Parliament

State Development, Natural Resources and Agricultural Industry Development Committee

July 2018

State Development, Natural Resources and Agricultural Industry Development Committee

Chair	Mr Chris Whiting MP, Member for Bancroft
Deputy Chair	Mr Pat Weir MP, Member for Condamine
Members	Mr David Batt MP, Member for Bundaberg
	Mr James (Jim) Madden MP, Member for Ipswich West
	Mr Brent Mickelberg MP, Member for Buderim
	Ms Jessica (Jess) Pugh MP, Member for Mount Ommaney

Committee Secretariat	
Telephone	+61 7 3553 6623
Fax	+61 7 3553 6699
Email	sdnraidc@parliament.qld.gov.au
Committee webpage	www.parliament.qld.gov.au/SDNRAIDC

Acknowledgements

The committee acknowledges the assistance provided by the Queensland Audit Office and the Department of Natural Resources, Mines and Energy.

Contents

Abbreviations

Auditor-General's report/ the Report	Auditor-General's Report 19: 2016-17 – Security of critical water infrastructure
DEWS	Department of Energy and Water Supply
DNRME	Department of Natural Resources, Mines and Energy
QAO	Queensland Audit Office

Chair's foreword

This report presents a summary of the State Development, Natural Resources and Agricultural Industry Development Committee's examination of the Auditor-General's Report 19: 2016-17 – Security of critical water infrastructure.

The committee's task was to consider the Auditor-General's findings as to whether a selection of entities responsible for critical water infrastructure had processes in place to protect their water control systems, and whether these entities could detect security breaches and restore systems in the event of an attack. The committee also examined the progress in implementing recommendations from the Auditor-General.

On behalf of the committee I thank the Queensland Audit Office and the Department for Natural Resources, Mines and Energy for their assistance with the committee's examination.

I commend this report to the House.

Chris Whiting MP

Chair

Recommendations

1 Introduction

1.1 Role of the committee

The State Development, Natural Resources and Agricultural Industry Development Committee (committee) is a portfolio committee of the Legislative Assembly which commenced on 15 February 2018 under the *Parliament of Queensland Act 2001* and the Standing Rules and Orders of the Legislative Assembly.[1]

The committee's areas of portfolio responsibility are:

- State Development, Manufacturing, Infrastructure and Planning
- Natural Resources, Mines and Energy, and
- Agricultural Industry Development and Fisheries.[2]

The committee has responsibility within its portfolio areas for:

The assessment of the integrity, economy, efficiency and effectiveness of government financial management by:

- examining government financial documents, and
- considering the annual and other reports of the Auditor-General.[3]

1.2 Role of the Auditor-General and Queensland Audit Office

The Auditor-General is an independent statutory officer appointed by the Governor in Council under the *Auditor-General Act 2009*. The Auditor-General is supported by the Queensland Audit Office (QAO).[4]

The Auditor-General undertakes both financial audits and performance audits of public sector entities. Financial audits provide an opinion on the financial statements of public sector entities, whilst performance audits address important aspects of public services, examining efficiency and effectiveness.[5]

1.3 Referral of the Auditor-General's report

Standing Order 194B provides the Committee of the Legislative Assembly shall as soon as practicable after a report of the Auditor-General is tabled in the Assembly, refer that report to the relevant portfolio committee for consideration.

A portfolio committee may deal with this type of referral by considering and reporting on the matter and making recommendations about it to the Assembly.[6]

On 8 August 2017 the Auditor-General's Report 19: 2016-17 – Security of critical water infrastructure was referred to the Public Works and Utilities Committee of the 55th Parliament.[7] That committee did not report before the dissolution of Parliament on 29 October 2017. The report was referred to the

---

1 *Parliament of Queensland Act 2001*, s 88 and Standing Order 194.

2 Schedule 6 of the *Standing Rules and Orders of the Legislative Assembly*, effective from 31 August 2004 (amended 15 June 2018).

3 *Parliament of Queensland Act 2001*, s 94(1)(a).

4 *Auditor-General Act 2009*, ss 6, 9.

5 See Queensland Audit Office: https://www.qao.qld.gov.au/our-role (accessed 20 June 2018).

6 *Parliament of Queensland Act 2001*, s 92(3).

7 Queensland Parliament, Record of Proceedings, 8 August 2017, p 2009.

State Development, Natural Resources and Agricultural Industry Development Committee on 3 May 2018.[8]

1.4 Examination process

The committee received a public briefing on the Auditor-General's report from the QAO and the Department of Natural Resources, Mines and Energy (DNRME) on 11 June 2018. The transcript of the public briefing is available from the committee's webpage.[9] The list of witnesses who appeared at the public briefing is at Appendix A.

Recommendation 1

The committee recommends that the Legislative Assembly note the contents of this report.

8 Queensland Parliament, Record of Proceedings, 3 May 2018, p 1000.

9 See https://www.parliament.qld.gov.au/work-of-committees/committees/SDNRAIDC.

2 Examination of the Auditor-General's report

2.1 Audit background

In Queensland, water service providers[10] monitor and control water transport, treatment and distribution. This includes the water distribution network for drinking water, reservoirs, and pump stations, and the collection and treatment of wastewater.[11]

Water control systems in Queensland have been maliciously targeted resulting in danger to public health and safety. The QAO identified attacks have resulted in overflows of untreated sewerage, reductions in water pressure, or shutdowns in the distribution of water.[12] As many of these systems are now connected to other networks and the internet, the risk of unauthorised access has increased.[13]

Water entities are responsible for securing their own water assets, however, several Australian Government entities play a role in setting guidelines and strategies for securing critical infrastructure, and assisting critical infrastructure owners when a security breach occurs.[14]

The safety and reliability of water supply in Queensland is governed by the *Water Supply (Safety and Reliability) Act 2008.*[15] Under this legislation safety relates to ensuring that there is a supply of water, rather than providing for information technology security. The legislation does not require guidance on information technology security to be provided to water entities.[16]

2.2 Audit objective and reasons

The Auditor-General's report was a performance audit to assess whether systems used to operate, manage and monitor water infrastructure were secure, and effective processes were in place to recover from adverse events.[17]

The audit was conducted because of the necessity for secure critical infrastructure, the 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.[18] The Auditor-General told the committee:

> *With the increase in reported attacks on critical infrastructure through information technology, we conducted an audit to assess how well a selection of water service providers is managing this risk. 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.*[19]

---

10 Queensland Audit Office, Security of critical water infrastructure, Report 19: 2016-17, (QAO, Report 19), June 2017, p 7.

11 QAO, Report 19, p 7.

12 QAO, Report 19, p 8.

13 QAO, Report 19, p 8.

14 QAO, Report 19, p 8.

15 At the time of the audit report the *Water Supply (Safety and Reliability) Act 2008* was administered by the Department of Energy and Water Supply. Following machinery of government changes, the Act is now administered by the Department of Natural Resources, Mines and Energy.

16 QAO, Report 19, p 9.

17 QAO, Report 19, p 34.

18 QAO, Report 19, p 34.

19 Public briefing transcript, Brisbane, 11 June 2018, p 1.

2.3 Audit conclusions

The audit found that water control systems were not adequately secure.[20] The age of many of these control systems, combined with more recent integration with corporate networks, had resulted in higher risks than previously recognised and tested for by the water service providers themselves. All entities audited were found to be susceptible to security breaches or hacking attacks because of weaknesses in processes and controls.[21]

The QAO audit found that attacks could disrupt water and wastewater treatment services.[22] An attack could lead to a risk to public health, appreciable economic loss in terms of lost productivity and could have a significant impact on the environment.[23]

The QAO acknowledged the efforts of the critical infrastructure owners, since the testing had occurred, to mitigate the risk of security incidents on their systems and to minimise the impact of such events.[24]

The entities audited 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 capability. Only one entity had documented its manual operating procedures, and none had ever tested running their whole plants manually.[25]

The QAO stated that the results of the audit serve as a timely reminder for any public sector entity managing critical infrastructure.[26] Entities should assess and strengthen defences to protect their systems from information technology and cyber threats, and ensure that manual operation of critical infrastructure is documented and well tested.[27]

2.4 Audit recommendations

The Auditor-General made four recommendations:

For the Department of Energy and Water Supply (DEWS):

1. Integrate information technology risks and cyber threats into the existing risk management framework for drinking water services and in the Queensland water and sewage service provider performance reports.
2. Facilitate information sharing about adopting standards for securing information technology amongst entities that manage water control systems.

For the entities audited:

3. Improve oversight, identification and monitoring of information technology risks and cyber threats to water control systems, including:
    - clearly articulating and assigning roles and responsibilities for all parties, including any external service providers in securing the systems
    - maintaining a complete and up-to-date list of assets for water control systems and assessing the risk exposure of each asset

20 QAO, Report 19, p 1.

21 QAO, Report 19, p 1.

22 QAO, Report 19, p 1.

23 QAO, Report 19, p 1.

24 QAO, Report 19, p 1.

25 QAO, Report 19, p 2.

26 QAO, Report 19, p 2.

27 QAO, Report 19, p 2.

- developing and implementing a security plan for water control systems based on risk assessments
- implementing appropriate user account access and authentication policies
- using a phased approach to implementing the Australian Government's 'essential eight' security controls based on each entity's risk assessment
- establishing performance indicators for security and periodically testing these controls to monitor the maturity and strength of defences built into the information technology control environment
- improving understanding of how to manage information technology risks and how they relate to other forms of operational risks.

4. Establish enterprise-wide incident response plans, business continuity, and disaster recovery processes for information technology, including:
    - testing the capability to respond to wide-scale information technology security incidents either through scenario testing or through desktop exercises
    - training staff to identify, assess, and have a coordinated response to information technology security breaches
    - adopting appropriate business continuity plans that include processes for reporting incidents to stakeholders and building on lessons learned
    - updating and testing information technology disaster recovery and business continuity plans to include processes to recover from a wide-scale information technology security breach
    - considering the impact of multiple system failures on business continuity planning and how entities can operate water and wastewater plans manually, if required.[28]

2.5 Committee consideration

In considering the Auditor-General's report, the committee held a public briefing with the QAO and DNMRE on 11 June 2018. The purpose of the briefing was to inform the committee of the key issues raised in the Auditor-General's report and to assess the progress in implementing the four recommendations.

2.5.1 Recommendations 1 and 2 of the Auditor-General

At the time of the audit the first and second recommendations of the Auditor-General's report were directed to the DEWS, however, following the machinery of government changes in 2018 these recommendations are now with the DNRME. Recommendations 1 and 2 related to suggested changes to risk management frameworks and performance reporting regimes, and the facilitation of information sharing of security standards.

The QAO advised the committee:

> *We did recommend in recommendations 1 and 2 for DEWS to integrate information technology risks and cyber threats into their existing risk management framework for drinking water services and in the Queensland water and sewerage service provider performance reports. That was one way in which we thought they could bring it into their existing frameworks rather than*

[28] QAO, Report 19, p 4.

> *requiring additional resources. Recommendation 2 is to integrate information sharing about standards for securing information technology.*[29]

At the briefing, the committee sought an update from DNRME in regard to the recommendations directed at them. The department advised that the implementation of the recommendations were dependent upon a better understanding of the potential cybersecurity threats as these threats were not uniform to all service providers. The committee was told that:

> *Providers of drinking water in Queensland range from small remote councils through to very large urban corporations. There are 85 registered drinking water service providers in Queensland and they operate over 300 individual supplies. An estimated 69 of the 85 providers operate services that supply fewer than 1,000 people which is approximately 300 to 400 connections. The largest provider in Queensland supplies drinking water to well over one million connections.*[30]

As a result of the diversity in water service providers, DNRME are currently undertaking a project to improve their understanding of potential weaknesses across the sector:

> *The project will gather information over a six-month period and is being implemented in partnership with a specialist contractor and six volunteer service providers… These providers represent different sizes and use a range of processes to manage their drinking water control systems… The data collected from the project and the other activities will be used to develop the process to integrate cyber-threats into the existing risk management framework and service provider performance outcome reporting.*[31]

Preliminary results from the project indicate that across various industries common cybersecurity vulnerabilities could be addresses at minimal cost by 'maintaining appropriate passwords, ensuring that program updates are installed, locking unattended computers and limiting physical access to buildings and water infrastructure'.[32] However, the committee was also told that the silo approach to water service provider's operations was a significant weakness in the security of their systems:

> *… one of the things that is most common is that the IT and the OT folks do not talk to each other or do not get together. Certainly, with the providers who we have spoken to, that has been one of the first things that they have been working on… There are lots of other aspects of their business that would need to be involved in that conversation that are not the drinking water folks—for example, finance and those sorts of people.*[33]

2.5.1.1 Recommendation 1

Recommendation 1 identified the need for DNRME to better 'integrate information technology risks and cyber threats into the existing risk management framework for drinking water services and in the Queensland water and sewage service provider performance reports'.[34]

The steps taken by the department to monitor how water entities are securing their water infrastructure, was discussed by the committee.[35] With regards to the implementation of actions in response to recommendation 1 of the Auditor-General, the department advised:

> *The drinking water quality management plan regulatory guidelines sets out the requirements for, among other things, the risk assessment process that drinking water service providers*

29 Public briefing transcript, Brisbane, 11 June 2018, p 3.

30 Public briefing transcript, Brisbane, 11 June 2018, p 5.

31 Public briefing transcript, Brisbane, 11 June 2018, pp 5-6.

32 Public briefing transcript, Brisbane, 11 June 2018, p 6.

33 Public briefing transcript, Brisbane, 11 June 2018, p 7.

34 QAO, Report 19, p 4.

35 Public briefing transcript, Brisbane, 11 June 2018, p 8.

(providers) must document in the drinking water quality management plan. A project to review all of our guidelines will commence on 20 June 2018. Information on cyber security risks will be informed by the Queensland Audit Office report and the department's current project into the risks of a broader range of service providers. The final requirements for cyber security for inclusion in the guidelines will be completed by the end of 2018.

The development of new key performance indicators is implemented through a technical working group with representatives of the department, a range of providers and industry bodies. The new key performance indicators will be developed by the end of 2018. The reporting timeframes for key performance indicators is annual and is based on financial years. Indicators are not changed half way through a reporting cycle and therefore the first data reported against the new cyber security indicators will be 1 October 2020 and will provide information on cyber security activities undertaken by providers between July 2019 and June 2020.[36]

2.5.1.2 Recommendation 2

The committee notes that the *Water Supply (Safety and Reliability) Act 2008* is implemented primarily through statutory guidelines. DNRME is responsible for monitoring ongoing engagement and the voluntary compliance of the regulated entities.[37] The department informed the committee:

We would prefer that they comply rather than us having to go out, for example, and issue a fine. There will be regulatory requirements, but our approach to regulation is to have the support system in place so that they can voluntarily comply—things like having fact sheets, templates for reporting, workshops and those sorts of things.[38]

Recommendation 2 identified the need for the DNRME to 'facilitate information sharing about adopting standards for securing information technology amongst entities that manage water control systems'.[39] The department outlined the implementation of actions in response to Recommendation 2:

The department proposes to work with other industry bodies such as the Local Government Association of Australia and Qldwater to raise awareness of the cyber security standards available and how they can be used and implemented by providers. The department's role in this work will be in the protection of drinking water quality and sewerage system performance. A suite of guidelines and standards have been identified by the Information Technology Security Expert Advisory Group of the Australian Commonwealth Governments Trusted Information Sharing Network for Critical Infrastructure Resilience and the Australian Signals Directorate. These activities commenced through the recent presentation by the department at the Queensland Water Directorate cyber security forum on 31 May 2018, which was attended by representatives from 24 providers. This work will be an ongoing activity.

As the department updates the regulatory guideline and develops the key performance indicators, supporting information will also be developed to assist providers to understand their regulatory obligations and encourage compliance. The existing key performance indicator reporting template and definitions / explanatory guide will be updated to include the new cyber security indicator information. These updates will occur simultaneously with the development of the indicators. The existing drinking water quality management plan guideline and template will be similarly updated. The department will also incorporate any learnings in regard to cyber

---

36 Department of Natural Resources, Mines and Energy, correspondence dated 18 June 2018, p 5.

37 Department of Natural Resources, Mines and Energy, correspondence dated 18 June 2018, p 6.

38 Department of Natural Resources, Mines and Energy, correspondence dated 18 June 2018, p 7.

39 QAO, Report 19, p 4.

security breaches and responses into existing supporting workshop programs and guidance material.[40]

Committee comment

Malicious targeting of Queensland's critical water infrastructure is a current and actual risk which will continue to increase with the increase use of technology operated systems. The committee is greatly concerned that departmental progress towards the recommendations of the QAO has not been timely and therefore to date limited.

The committee notes the recent DNRME progress made in the implementation of the QAO recommendations and that a number of actions will not be delivered by the original deadline of the end of 2018. Given the importance of the matters raised in the QAO report the committee requests that DNRME provided an update on the implementation of Recommendations 1 and 2 by the end of June 2019.

Recommendation 2

The committee recommends that the Department of Natural Resources, Mines and Energy provide a briefing/written briefing to the committee by the end of June 2019 on its implementation of the Auditor-General's Recommendations 1 and 2 in the Auditor-General's Report 19: 2016-17 Security of critical water infrastructure.

2.5.2 Recommendations 3 and 4 of the Auditor-General

Recommendations 3 and 4 of the Auditor-General's report were addressed to the entities that were the subject of the audit. Given the nature of the audit and the fact that these entities were not named the committee did not directly seek evidence from them. However, the QAO advised the committee:

We did find that the entities were really proactive. As we were doing the audits they were improving their control environments as we went through. When we got their responses they all undertook to improve their planning. You will notice in the report that we found that identification of risks was an issue at the time. Once they identified the risks they were very happy to address those risks. The intention was there to make sure they have a good security environment. It is those things that we identified that they were willing to correct.[41]

DNRME provided the committee with information relating to a number of water entities and the steps they have taken to improve the protection of critical water infrastructure.[42]

Committee comment

The committee notes that many water service providers, historically, have not paid sufficient attention to the potential vulnerabilities to their water infrastructure. However, the committee is encouraged by the willingness of water entities to address identified weaknesses and develop comprehensive management approaches to protect Queensland's critical water infrastructure. The committee acknowledges the constructive responses of the water entities both during and after the audit.

2.6 Monitoring the implementation of Auditor-General recommendations

The committee sought to identify what monitoring had taken place in regard to the implementation of recommendations contained within the Report.[43] The QAO advised the committee:

---

40 Department of Natural Resources, Mines and Energy, correspondence dated 18 June 2018, p 5.

41 Public briefing transcript, Brisbane, 11 June 2018, p 2.

42 Department of Natural Resources, Mines and Energy, correspondence dated 18 June 2018, pp 2-4.

43 Public briefing transcript, Brisbane, 11 June 2018, pp 2-3.

> *We have not been back to all of the entities that we audited but there is one entity that reports to us periodically about the work that they are doing.*[44]

Additionally, the QAO advised:

> *After a performance audit we do sometimes have entities who proactively engage with us. They come to us and want to report progressively on how they are implementing our recommendations, but that is them coming to us in that form … As part of our strategic audit planning, when we are working out the agenda for the portfolio of audits for the next 12 months and then the following two years after that, we do write out to audits usually about two years previous and get them to self-report where they are up to with implementing our recommendations. Then we look at all of those to see, when we only do one to two per year, which ones might be the most valuable for us to get back in to have a look and do a full-blown performance audit, where we actually audit the effectiveness of the implementation of that recommendations and not just whether they have done it or not.*[45]

Committee comment

The committee notes that the QAO does not systematically or formally monitor the implementation of recommendations made in its reports. However, QAO recommendations can be monitored through the QAO's strategic audit planning process and the work of portfolio committees. The committee considers that there may be a need to improve the monitoring of the implementation of QAO recommendations to ensure the full value of Auditor-General reports are realised.

The committee commends the QAO for their significant contribution to public sector performance.

44 Public briefing transcript, Brisbane, 11 June 2018, p 2.

45 Public briefing transcript, Brisbane, 11 June 2018, p 3.

Appendix A – Officials at public briefing on 11 June 2018

Queensland Audit Office

- Mr Brendan Worrall, Auditor-General
- Ms Daniele Bird, Deputy Auditor-General
- Mr Darren Brown, Director, Performance Audit
- Ms Mayus Nath, Director, Information Systems Audit

Department of Natural Resources, Mines and Energy

- Ms Toni Stiles, Director, Water Supply Regulation, Operations Support
- Ms Amanda Downes, Executive Director, Operations Support, Natural Resources
- Mrs Susan Larsen, Manager, Planning, Review and Improvement, Operations Support