STATE DEVELOPMENT, NATURAL RESOURCES AND AGRICULTURAL INDUSTRY DEVELOPMENT COMMITTEE

Members present:

Mr CG Whiting MP (Chair)
Mr DJ Batt MP
Mr JE Madden MP
Mr BA Mickelberg MP
Ms JC Pugh MP
Mr PT Weir MP

Staff present:

Dr J Dewar (Committee Secretary)
Ms N Mitchenson (Assistant Committee Secretary)
Mr M Binns (Inquiry Secretary)

PUBLIC BRIEFING—AUDITOR-GENERAL REPORT NO. 19: 2016-17—SECURITY OF CRITICAL WATER INFRASTRUCTURE

TRANSCRIPT OF PROCEEDINGS

MONDAY, 11 JUNE 2018

Brisbane

MONDAY, 11JUNE 2018

_____

The committee met at 10.33 am.

CHAIR: Good morning. I declare open the public briefing on the Auditor-General's report No. 19 of 2016-17, *Security of critical water infrastructure*. The Committee of the Legislative Assembly referred this report to the State Development, Natural Resources and Agricultural Industry Development Committee for its consideration. Thank you for your attendance here today. I note that a public briefing on this report was previously held in the 55th Parliament, so the committee appreciates your attendance again. I am the member for Bancroft and chair of the committee. The other committee members here with me today are Mr Pat Weir, the deputy chair and member for Condamine; Mr David Batt, the member for Bundaberg; Mr Jim Madden, the member for Ipswich West; Mr Brent Mickelberg, the member for Buderim; and Ms Jess Pugh, the member for Mount Ommaney.

The committee's proceedings are proceedings of the Queensland parliament and are subject to the standing rules and orders of the parliament. Witnesses should be guided by schedules 3 and 8 of the standing orders and note that their responsibility is to provide factual and technical background to government legislation and administration. Those here today should note that these proceedings are being broadcast to the web and transcribed by Hansard. Media may be present so you may also be filmed and photographed. Before we commence could you please switch off your mobile devices or put them on silent. I now welcome the Queensland Audit Office for this briefing.

BIRD, Ms Daniele, Deputy Auditor-General, Queensland Audit Office

BROWN, Mr Darren, Director, Performance Audit, Queensland Audit Office

NATH, Ms Mayus, Director, Information Systems Audit, Queensland Audit Office

WORRALL, Mr Brendan, Auditor-General, Queensland Audit Office

CHAIR: Would one of you like to make an opening statement?

Mr Worrall: Thank you, Chair, for the opportunity to brief the committee on our report on the security of critical water infrastructure which we tabled in June 2017. As this audit is of a sensitive nature because it goes to the security of one of our critical infrastructure sectors, we would like to ask for a private briefing if we are not able to answer some of the questions.

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.

Because the Australian government considers water infrastructure as critical, there is a wide policy platform that crosses both national and state levels. Several entities develop guidelines for designing security within systems and play a role in assisting agencies in responding to threats. However, we found that the water control systems we audited were not as secure as they could have been when we did the audit. The security controls that the entities implemented were not sufficient to protect the systems from internal and external threats. At the time of our audit all entities we audited were susceptible to hacking attacks, and these attacks could disrupt water and wastewater treatment services. They could also disrupt other services that relied on the entity's IT environment. A sewage spill such as in the Maroochy shire in the year 2000 could significantly impact the environment.

The entities we audited have since taken action to mitigate the risks we highlighted and to improve their security controls. In addition, all entities we audited had the capability to respond to information technology incidents if they detected them. They could also operate their smaller plants or parts of the larger plant manually, but they were not well prepared to respond to a cyber attack because they had not tested their responses from a malicious intent that occurs without notice and

affects several systems at the same time. The result of this audit serves as a timely reminder for any public sector entity managing critical infrastructure to assess and strengthen defences to protect their systems from IT and cyber threats. We are happy to take questions.

CHAIR: We appreciate you coming back to brief a committee again on this. Obviously there have been some improvements or some changes made since you reported previously. Could you perhaps provide an update on what has occurred since the last time you briefed us? Have the improvements been made or have these entities taken salient notice of what has been in the report previously?

Ms Nath: 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. They have developed some implementation plans for security controls and they have implemented some of the controls as well. They currently have a security plan in place and they are working through and improving the security environment. We have done audits of financial systems since we did this particular audit and we are finding that those entities are improving their controls over the security in terms of their financial systems.

Ms Bird: In terms of this report, considering it is a 2016-17 report it has not formed part of our follow-up processes yet. As we have briefed the committee previously, as part of doing our strategic order planning every year, we come back when we are visiting our three-year rolling plan so it will form part of this next 12 months progress report, where we write out to the entities that were a part of this audit and get them to self-report—so it is not us auditing them—where they are up to with the recommendations and then we will use that to select whether we do a follow-up audit on this particular one. Cybersecurity is, however, in the current strategic audit plan for 2018-2021—so not particularly following up this audit but cybersecurity in general for the public sector is on our strategic audit plan for this financial year.

CHAIR: One particular organisation you have worked with on cybersecurity is making progress, and obviously you will come back and look at the financial part of that audit as well, but otherwise we have to wait until the next rolling part to see how well they have implemented it?

Ms Bird: Yes. A follow-up audit entails doing a full blown audit on the recommendations that we made in this report and looking at how well they have implemented them, so not just a self-report. We do not do a follow-up on 100 per cent of our performance audits so there is no guarantees we will definitely do that, but we will certainly consider it as part of our next round of looking at which ones we do. For instance, this year we are doing one on the bushfire report.

Mr WEIR: You mentioned that there are federal guidelines around water security. Obviously other states are in the same predicament, trying to follow those guidelines. How does Queensland rate against those? Is there any way we can measure how we stand against other states?

Ms Nath: We are not able to measure the security posture of other states or other entities for that matter because everyone keeps it close to their heart in terms of how well they have secured their environments. We can do audits of our own entities—Queensland government organisations. When we did the audit of traffic light systems, which were in the same area, which was the SCADA systems or the engineering systems that we audited for the water, we found that there were similar types of issues and there were some basic levels of control that were not in place at that time. We find that entities can actually do a lot better in strengthening their cyber resilience.

Ms Bird: The last time we were before the previous committee the question came up around reporting to a national body which would give you, as you are rightfully asking, that comparative information. We looked into that post the committee as a question on notice and we could not see that there was any calling for mandatory reporting to that national body at the moment.

Mr MADDEN: I note in your report you say that following your testing the entities made efforts to mitigate the risk of security incidents. I wonder if you could provide a bit more detail about that. Could you also advise the committee if you are satisfied with their response?

Ms Nath: 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.

Mr MADDEN: Thank you.

Ms Nath: It was a major undertaking to look at their overall environment. That is why they all needed to have plans for implementing it and strengthening it progressively. The other idea was to make sure that they are on the lookout for new and emerging threats so that they are on the front foot with new risks that come up.

Mr BATT: In your report, under 'Audit findings' the first dot point discusses that 'several Queensland government departments deal with counter-terrorism and response, but no central agency is responsible for supporting critical water infrastructure owners to protect these systems from security events resulting from information technology risks'. It seems that where you have multiple departments and agencies working is where things do slip through the cracks. Did you have any recommendations or ideas on how that could work better?

Ms Nath: Yes. The key thing we found was that there were so many good standards available. People could use those to design their security from scratch when they were implementing their systems but not everybody was aware of those standards. We thought that at the state level we do not have a central body that coordinates all of this and makes sure that critical infrastructure owners are aware of good security designs and are addressing, identifying and managing their risks. When we talked to the QCGIO at the time, they looked at more the internet and corporate network type system, whereas the engineering and the SCADA systems that deal with critical infrastructure are of a different nature and their standards are significantly different from how you would secure your internet type protocols. They did not have the mandate to be looking at critical infrastructure.

We looked at DEWS at the time. DEWS was administering the water safety act. That talked about the safety of supply of water but not really about the safety and security of IT systems and assets that are used to manage the supply of water. We did recommend in recommendations 1 and 2 for DEWS to integrate information technology risks and cyberthreats 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 requiring additional resources. Recommendation 2 is to integrate information sharing about standards for securing information technology.

Ms PUGH: You have spoken before about your engagement with the different entities that you have audited. You alluded to some kind of ongoing contact in that they have been quite proactive. Could you outline what contact you have between that initial audit and then any potential follow-up audits and how you might select the entities that may be candidates for follow-up audits?

Ms Bird: As Mayus has indicated, 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. These are all public sector entities, so we have financial auditors who attend audit committees as well each year. They will sometimes hear about the update to recommendations through audit committees or, alternatively, sometimes throughout the financial audit. The purpose of a financial audit is not to follow up on a performance audit recommendation. In this instance we are talking about very different systems to when you are looking at the infrastructure system. We have had, as Mayus indicated, one entity that has selected to proactively inform us about what it is doing.

On the follow-ups, as I indicated, each year we would generally do about 10 new performance audits and one or two follow-up audits, where we go back to a previous report and do a full-blown audit. 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 recommendation and not just whether they have done it or not.

Mr MICKELBERG: Given the attack in 2000 on the Sunshine Coast which you mentioned—I find the lack of control that exists within these public entities astounding—did each of the entities that you audited have a specific individual responsible for security of the critical water infrastructure within their entity?

Ms Nath: No. All of the entities that we audited had information security officers. They were responsible for overall information security. One of the key elements that we found was the lack of integration between something that they call OT, which is operational technology, which is the critical infrastructure, versus IT, which is the corporate systems and corporate networks. They were not working together. They were not integrating well. That was a key factor in things slipping through the

cracks. The IT information security officers would be quite well versed in securing the IT environments, whereas the OT people, the engineers who were running the SCADA systems, probably were not as well versed.

There is a reason for this. When they first implemented the engineering systems they used to be secluded and isolated from the corporate networks and from the internet and from everything else. It was just this little thing that someone was running. Now we are connecting all of these things up on the corporate networks. We wanted information out of it. We want to be able to use the internet on various devices, and robotics, automation and all of these things are coming in. It is good to use all of these technologies but at the same time we need to upskill in terms of how we secure them.

Mr MICKELBERG: Noting there is a significant divergence in the size and sophistication of the entities you audited, did the larger entities that you audited have dedicated individuals with security, both IT and physical security?

Ms Nath: Are you talking about operational technology?

Mr MICKELBERG: What I am concerned with is that an individual at some level in the organisation is responsible for implementing the appropriate controls in this area. Does an entity that is of an appropriate size—your Unitywaters, your Seqwaters, your South-East Queensland councils—have an individual or a group of individuals who are responsible for ensuring that these measures are implemented and that appropriate controls are put in place?

Ms Nath: Around the IT and corporate side, yes; around OT, no.

CHAIR: Member for Buderim, that was one of the questions I was going to ask of the department, so we will pursue that then. Thank you very much. There being no further questions, we will conclude this briefing from the Queensland Audit Office.

DOWNES, Ms Amanda, Executive Director, Operations Support, Natural Resources, Department of Natural Resources, Mines and Energy

LARSEN, Mrs Susan, Manager, Planning, Review and Improvement, Operations Support, Department of Natural Resources, Mines and Energy

STILES, Ms Toni, Director, Water Supply Regulation, Operations Support, Department of Natural Resources, Mines and Energy

CHAIR: I now welcome officers from the Department of Natural Resources, Mines and Energy to this briefing. Would you like to make an opening statement?

Ms Stiles: Thank you for the opportunity to brief the committee today. The Queensland Audit Office report *Security of critical water infrastructure* was delivered to parliament in June 2017 and recommended that the then department of energy and water supply, now the Department of Natural Resources, Mines and Energy, integrate information technology risks and cyberthreats into the existing risk management framework for drinking water services and into the Queensland water and sewerage service provider performance reports; and also facilitate information sharing about standards for securing information technology amongst entities that manage water control systems. The department acknowledges that cybersecurity can represent a threat to water quality such as through malicious actions to alter chemical dosing. The department fully supports the report recommendations and plans to implement the recommendations by the end of 2018 in line with the time frames tabled in the QAO report to parliament.

The existing regulatory system under the Water Supply (Safety and Reliability) Act 2008 is based on risk assessments and drinking water quality management plans and requirements for drinking water and sewerage providers to report annually on performance outcomes such as financial sustainability, customer service, water and sewerage infrastructure and water supply continuity. Taking into account the time frame stipulated in the act for drinking water quality management plan amendments and performance outcome reporting, the requirements introduced in response to the QAO report recommendations will commence in mid-2019. Further work is, however, necessary before the recommendations can be fully implemented. The department is committed to ensuring that its response to the recommendations provides a cost-effective and meaningful result for government and providers whilst still improving cybersecurity protections.

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. Additionally, the department has received over 2,000 water quality incidents since 2009, when the drinking water regulation was introduced. The cause of these incidents ranges from microbiological and chemical contamination to events such as infrastructure failure, overdosing and loss of water supply. None of these incidents has been linked to the security of information technology or cyberthreats.

The QAO audited three large urban water service providers. Larger providers are more likely to be vulnerable to security related issues as they, by necessity, operate more technologically sophisticated systems. Our data indicates that the use of technology varies greatly amongst providers of these services; hence their susceptibility to information technology and cybersecurity breaches is likewise varied.

The successful implementation of the QAO audit recommendations is dependent on a better understanding of these vulnerabilities across that scope of providers to cybersecurity issues and developing solutions that result in improved protections from cybersecurity threats for all providers and the public. The department is undertaking a project to improve our understanding of these vulnerabilities. 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. The providers participating in the project are the councils for Townsville, Burdekin, Charters Towers, Banana, Redland and Livingstone. These providers represent different sizes and use a range of processes to manage their drinking water control systems.

The department will undertake further work to summarise the processes and controls used by very small providers. Many of these providers rely on manual processes and have very little technical integration. The cybersecurity risks associated with these very small providers will be established on the basis of the data obtained from the project that I have previously mentioned.

The preliminary results from the project indicate that common cybersecurity vulnerabilities across various industries can be remediated at minimal cost. These include things such as maintaining appropriate passwords, ensuring that program updates are installed, locking unattended computers and limiting physical access to buildings and water infrastructure. The data collected from the project and the other activities will be used to develop the process to integrate cyberthreats into the existing risk management framework and service provider performance outcome reporting.

The Water Supply (Safety and Reliability) Act 2008 is implemented primarily through statutory guidelines. These guidelines provide the necessary detail to set regulatory standards and they are flexible enough to account for emerging hazards such as cybersecurity. However, any changes to these guidelines will be consulted on widely with the water supply industry prior to implementation.

Following the implementation of the QAO recommendations, the department will be responsible for ongoing compliance monitoring to ensure that the requirements are being met. Appropriate support and education will be provided by the department for our regulated entities to facilitate voluntary compliance. The implementation of the information-sharing recommendation in the report has commenced. On 31 May this year the department joined a number of other presenters, including two of the providers included in the QAO audit, to present information at an industry forum. The forum was focused on raising awareness of cybersecurity in the water supply industry, providing guidance on how to integrate cybersecurity into everyday business, updating the progress of activities undertaken thus far and detailing how the recommendations from the QAO audit are being addressed.

In summary, cybersecurity is an emerging threat to water quality and service provider performance. The department is committed to working with providers to better understand how this threat can be managed, share information and ensure an appropriate level of accountability through regulation.

CHAIR: There are a lot of attention-grabbing parts in this report. When you have talked to them, have these entities appreciated the gravity of the potential risks they face? Firstly, are they taking on that message?

Ms Stiles: Based on the engagement that we have had with the entities, I think they understand that this is an emerging hazard. There is just the unknown of what they can do to manage it, how big the risk is and how they integrate that into the other hazards that they have to consider in terms of water quality. My feeling is that absolutely they believe that this is a serious issue that they have to address.

CHAIR: We have talked about plans and strategies that are happening over a six-month and longer period. As this is an emerging and present threat, have they taken any action immediately? What are the most pertinent actions they have taken immediately, whether that be employing people with specific knowledge or changing what they do? Is there any specific action that they have taken immediately to address these things?

Ms Stiles: The difficulty for us is that we do not own these services, so we do not have an understanding of how they look at activities such as this, particularly given that they are broader than just providing drinking water. I mentioned that two of the providers who presented at the forum have taken considerable actions to address the recommendations and, indeed, have put on specific people to address that in an ongoing way. In a lot of the service providers, particularly the small ones, there just was not the awareness. That is something that we are having to build as we are doing the project.

Mr WEIR: You talk about different IT services in different areas. Is there a universal IT service that could be used across the whole state that would be easier to manage? It seems that it is all a bit higgledy-piggledy. Some entities would have higher security than others and they are better able to manage it.

Ms Stiles: I think it is very much dependent on a lot of things. There are places that do not, for example, have the internet availability that would provide the level of technical integration that some other services have. It is just not practical. It is not available. It is dependent on staff numbers.

There is a common system—a SCADA system—that is used predominantly throughout the water industry but, again, it has varying levels of integration back into the broader business. Then it is customised depending on things like the water quality that is coming into treatment plants, for example. There are lots of reasons they are different and why they have different levels of integration.

Mr WEIR: There is no IT provider out there?

Ms Stiles: Not that I am aware of that you could apply across the drinking water industry.

Ms PUGH: You have covered the fact that there are 300 entities of vastly different sizes and scale. I want to understand your ongoing communication with the entities going forward. I imagine that what might be relevant for one in the south-east corner in terms of their security and what is achievable is not for something in Cunnamulla, for example. Are you able to tell us how you are tailoring your approaches to the larger entities versus the smaller entities so that they can all get the best outcome?

Ms Stiles: That was part of the idea of doing the project. It was to work out if there is a differing vulnerability among the different sizes of service providers and then supplement that with work on the very small providers. In the process of making amendments to our statutory guidelines, we have an advisory committee that is made up of a number of different service providers from around the state. We find that that is quite a good way to get that representative view about what is practical and what can be done and work out the happy medium—or is it different requirements for different sizes? We need to look at all of those things as we go forward.

Mr BATT: You mentioned a few times that this is an emerging hazard. I think it is a current hazard. We had an attack many years ago. It is something that we need to be dealing with sooner rather than later. Ms Stiles, you mentioned that these organisations could come in under voluntary guidance. Did you say that before?

Ms Stiles: No, voluntary compliance. 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.

Mr BATT: Under the act they report to you and if they do not voluntarily comply then you could make them comply?

Ms Stiles: Correct.

Mr BATT: You just mentioned the IT versus the SCADA system. Are you ensuring that those entities are looking to combine their systems so that someone is overviewing all of those systems? From my background, I can understand that the IT people did one part and the engineers looked after the SCADA, but that needs to be overviewed by someone.

Ms Stiles: It is one of the first things. The specialist contractor we engaged to help us on this project said that 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. As an example, one of the providers has instigated a committee where the IT and the OT people get together to talk about how they can manage their systems better. 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.

Mr MADDEN: Your report notes that the Australian government guidelines require the state government to assist critical infrastructure owners to implement security controls. Can you give us an outline of those Australian government guidelines?

Ms Stiles: From what I understand, there are quite a few guidelines that are being used by the entities. The national draft legislation is aimed at the very large providers and there is some reporting associated with very large providers, but I do not know of the applicability of those guidelines across the broader water industry at this point.

Mr MICKELBERG: I am also concerned about your language in saying that this is an emerging risk. It is clearly an actual risk. Eighteen years ago this risk existed in South-East Queensland. It concerns me that management has not paid an appropriate level of attention to this issue—things like KPIs, comprehensive risk assessments and implementing controls. Is it fair to suggest that the management of these entities are not paying an appropriate level of attention to the security of these water assets?

CHAIR: Would you like to put that in a different way?

Mr MICKELBERG: I am not allowed to ask you if it is fair. I will rephrase it. Have you identified instances post this audit being completed where management continues to fail to pay appropriate attention to things like KPIs, comprehensive risk assessment, the implementation of those—

CHAIR: Member for Buderim, try for a third time.

Mr MICKELBERG: No, I will let that stand.

CHAIR: I might have to rule that out of order.

Mr MICKELBERG: On what basis?

CHAIR: Bear in mind when we started this briefing we talked about issues regarding sensitivity and security. I do not want our public servants saying on the record that they agree or do not agree that other agencies have failed in this cybersecurity instance, hence I am asking you for a third time—

Mr MICKELBERG: My question is quite simple: has management paid an appropriate level of attention to implementing security controls in their entities—yes or no?

CHAIR: This impinges on issues of security. We are going to have a private meeting to deal with this issue.

Proceedings suspended from 11.13 am to 11.21 am.

CHAIR: We will now resume our public hearing. I believe the member for Buderim has a question.

Mr MICKELBERG: I will rephrase my previous question. Can you provide the committee with evidence of what each of the large water entities is doing to improve its protection of critical water infrastructure and what the department is doing to monitor how these entities are securing their water infrastructure? I would like a bit of detail in this answer, so I am happy for you to take the question on notice and provide that to the committee subsequently if you deem that appropriate.

Ms Stiles: In terms of what each of the 84 is doing or—

Mr MICKELBERG: There are likelihoods and consequences involved, so we are predominantly concerned with the larger entities that have a greater capacity to control and make efforts in this space. If you want to restrict yourself to those larger entities, that would be fine.

Ms Downes: Can we clarify that the larger entities we would seek information from would be the three as part of the audit?

Mr MICKELBERG: We can provide you with a list. My view would be that it would be Seqwater, Unitywater and your local municipal councils in the south-east in terms of their sewerage and that sort of thing, but we are not talking about Indigenous councils or small town councils.

CHAIR: I think we are also looking at the larger eastern seaboard cities as well: Cairns, Townsville, Mackay, Rockhampton and Bundaberg.

Ms Downes: We can certainly ask the question of the providers.

Mr MICKELBERG: We are also keen to know what the department is doing in this space to monitor their response to the Audit Office's report.

Ms Downes: Yes.

CHAIR: There is another question on notice. You have a number of issues that need to be completed by the end of quarter 4 of 2018. That includes the water quality management plan, management framework, cybersecurity related key performance indicators, annual reporting framework, standards framework and guidance resources. The question on notice is: will those dot points be completed by the end of quarter 4 of 2018?

Ms Downes: Yes, will do.

CHAIR: Added to that, can you give an update of where you are with those particular dot points?

Ms Downes: Yes.

CHAIR: Answers to questions on notice are to be provided by 10 am on Monday, 18 June. The time for questions has now expired. Thank you very much for your attendance.

The committee adjourned at 11.24 am.