REPORT FOR ACTION WITH CONFIDENTIAL ATTACHMENT

Toronto Water SCADA System Security: Results of the Follow-up of Previous Audit Recommendations

Date: February 4, 2022
To: Audit Committee
From: Auditor General
Wards: All

REASON FOR CONFIDENTIAL INFORMATION

Confidential Attachment 1 to this report involves the security of the property of the City of Toronto.

SUMMARY

The Auditor General has proactively raised concerns about evolving cybersecurity threats to the City and its Agencies and Corporations. These threats are real and large-scale attacks have disrupted public services in jurisdictions across North America and around the world, such as emergency response systems, utility services and law enforcement operations.

A SCADA system[1], also known as an Operational Technology (OT) system, is used to control industrial processes at facilities like water and wastewater treatment plants and at energy, utilities and transportation facilities. Toronto Water uses this system to manage and control critical infrastructure equipment and processes used in the treatment and distribution of water.

Recognizing the need to protect critical water assets, the Auditor General initiated an audit of the SCADA system in 2019 and expedited the follow-up review of the audit recommendations in 2021. The 2019 audit was the Office's first critical infrastructure audit of the City's Operational Technology (OT) systems[2].

The objective of the 2021 follow-up review was to assess the adequacy of controls in place to address potential threats to the SCADA network, systems and applications, and to review actions taken by management since the 2019 audit. The Auditor General

[1] https://csrc.nist.gov/glossary/term/supervisory_control_and_data_acquisition (SCADA)

[2] https://www.toronto.ca/legdocs/mmis/2020/au/bgrd/backgroundfile-145342.pdf

made 11 confidential recommendations in the 2019 SCADA audit. Given the importance of critical infrastructure systems and evolving cybersecurity threats, the Auditor General re-tested the controls to verify the implementation of recommendations.

At the November 2021 Audit Committee, we provided our public report and a high-level confidential presentation on the implementation status of the recommendations[3]. During our follow-up review, we determined that seven recommendations are fully implemented. An overview of the results is contained in Attachment 1. The details of management actions on each confidential recommendation are presented separately to this report in Confidential Attachment 1.

RECOMMENDATIONS

The Auditor General recommends that:

1. City Council direct that Confidential Attachment 1 to this report from the Auditor General be released publicly at the discretion of the Auditor General, after discussions with the appropriate City Officials.

FINANCIAL IMPACT

Implementing the recommendations to strengthen both physical security and cybersecurity controls at Toronto Water facilities would assure the supply of safe drinking water to the citizens of Toronto.

The extent of costs and resources needed to implement the recommendations is not determinable at this time. The investments needed to improve controls to manage and respond to cyber threats likely offsets the costs that could result from security breaches, which could include recovery of infrastructure systems, data recovery/cleanup, financial loss, reputation damage, fines and litigation.

DECISION HISTORY

In 2019, the Auditor General initiated an audit of the Toronto Water SCADA system. The report was tabled at the February 10, 2020 Audit Committee meeting. City Council's decision is available at:

http://app.toronto.ca/tmmis/viewAgendaItemHistory.do?item=2020.AU5.6

At the November 2, 2021 Audit Committee meeting, the Auditor General provided a public report with a high-level confidential presentation on the implementation status of

[3] https://www.toronto.ca/legdocs/mmis/2021/au/bgrd/backgroundfile-172299.pdf

the recommendations regarding the Toronto Water SCADA system. City Council's decision is available at:

http://app.toronto.ca/tmmis/viewAgendaItemHistory.do?item=2021.AU10.5

The Auditor General will continue to follow up the implementation status of cybersecurity recommendations and update Council on actions taken by management to address potential cybersecurity risks.

COMMENTS

The City uses a supervisory control and data acquisition (SCADA) system to manage drinking water treatment and wastewater treatment plants. These are critical infrastructure assets and must be protected.

In this follow-up review, we completed a cybersecurity vulnerability assessment, penetration testing and physical security assessment of selected water plants.

The procedures and work performed for this report do not constitute an audit in accordance with Generally Accepted Government Auditing Standards (GAGAS). However, we believe the work performed and information gathered provide a reasonable basis for our findings, conclusions and recommendations.

We express our appreciation for the coordination of management comments by the staff and management of the Toronto Water Division, Technology Services Division and the Office of the Chief Information Security Officer.

CONTACT

Syed Ali, Audit Director, IT & Strategy, Auditor General's Office
Tel: 416-392-8438, Fax: 416-392-3754, E-mail: Syed.Ali@toronto.ca

Suzanna Chan, Audit Manager, Auditor General's Office
Tel: 416-392-8033, Fax: 416-392-3754, E-mail: Suzanna.Chan@toronto.ca

SIGNATURE

Beverly Romeo-Beehler
Auditor General

ATTACHMENTS

Attachment 1 – Toronto Water SCADA System Security: Results of the Follow-up of Previous Audit Recommendations

Confidential Attachment 1 – Results of the Follow-up of Previous SCADA Audit Recommendations