# REPORT FOR ACTION WITH CONFIDENTIAL ATTACHMENT

# Toronto Police Service IT Infrastructure: Cybersecurity Assessment and Follow-up of Previous Recommendations

**Date:** June 26, 2025
**To:** Toronto Police Services Board
**From:** Auditor General
**Wards:** All

## REASON FOR CONFIDENTIAL INFORMATION

This report involves the security of property belonging to the City or one of its agencies and corporations. Confidential Attachment 1 to this report is explicitly supplied in confidence to the Toronto Police Service which, if disclosed, could reasonably be expected to impact the safety and security of the City, its services, and residents.

## SUMMARY

The Toronto Police Service (TPS) uses its Information Technology (IT) Infrastructure to help deliver mission critical work to keep the City's communities safe.

This report is a follow-up to the first TPS cybersecurity assessment completed by the Auditor General in 2021, following a request from the Toronto Police Services Board.

Cybersecurity incidents do not only impact recovery, response, and remediation costs, but also cause significant indirect costs in the form of disrupted operations as well as reputational damage. It is therefore essential that organizations have robust cybersecurity measures in place. Protecting the TPS's IT infrastructure is important to not only prevent costly outages and breaches, but to maintain public confidence in the organization's ability to respond to residents' calls for service and protection.

This public report contains three recommendations. The confidential findings and recommendations to improve TPS cybersecurity are presented separately to this report in Confidential Attachment 1. In addition, a detailed technical report has also been provided to management for expediting actions.

Management agrees with the recommendations contained in the confidential attachment to this report, which also includes management's response.

## RECOMMENDATIONS

The Auditor General recommends that:

1. The Board receive the public report and Confidential Attachment 1 from the Auditor General.

2. The Board direct that all information contained in Confidential Attachment 1 to this report remain confidential.

3. The Board forward this public report to City Council through the City's Audit Committee for information.

## FINANCIAL IMPACT

Implementation of the recommendations contained in Confidential Attachment 1 will further improve the Toronto Police Service's cybersecurity posture. The extent of costs and resources needed to implement the recommendations is not determinable at this time. The investment needed to improve controls to manage and respond to cyber threats offsets the potential costs resulting from security breaches, which could include data recovery/cleanup, financial loss, reputational damage, fines, or litigation.

## DECISION HISTORY

In December 2019, the Toronto Police Services Board requested the Auditor General conduct a cybersecurity assessment at the TPS. The Auditor General completed her assessment in 2021 and tabled her report at the June 24, 2021 TPS Board meeting. The 2021 report included recommendations for management to improve cybersecurity at TPS, including a request for the Auditor General to perform follow-up work.

The Auditor General started this follow-up review in 2024, and it is part of the 2025 Work Plan. The 2025 Audit Work Plan is available at: https://www.toronto.ca/legdocs/mmis/2024/au/bgrd/backgroundfile-250975.pdf.

## COMMENTS

With cybersecurity threats evolving across the globe, the City of Toronto and its agencies and corporations must ensure their cybersecurity programs are adapting to

new challenges and threats. It is important for the TPS to continue with its efforts to keep pace with the evolving demands from the rapidly shifting digital landscape.

Over the past few years three major city agencies, the Toronto Transit Commission, Toronto Zoo, and Toronto Public Library, have been affected by operationally disruptive cyberattacks. Cyber crime is global in nature, making it difficult to combat; a recent Interpol operation to shut down cyber criminals operating phishing, malware and ransomware attacks involved 60 law enforcement agencies and 50 member countries, including Canada.[1]

**Notable cyberattacks on police agencies**

Police agencies and at times, their associated vendors, continue to be the target of cybersecurity threats. Recent notable examples include:

- Royal Canadian Mounted Police (RCMP) – was targeted by a cyberattack in 2024.[2] This followed a 2023 ransomware attack on an RCMP subcontractor which compromised the privacy of some employees.[3]
- Australian Federal Police – Personal details of Australian Federal Police officers were leaked following the 2023 hack of an Australian law firm by a Russian-linked ransomware group.[4]
- Tanzanian National Police – The national police service's social media account was hacked in May 2025 to spread misinformation including a false report of the death of the country's president.[5]

As cybersecurity threats expand and evolve, it is important that the Auditor General continues her cybersecurity assessments so that she can continue to make recommendations to improve security controls across the City, and its agencies and corporations.

Given the services TPS provides, the extent of personal and highly sensitive data it holds, and the critical infrastructure the organization supports, it must prioritize protecting its systems against cyberattacks and adapt to emerging threats. The confidential findings and recommendations are contained in Confidential Attachment 1.

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

We express our appreciation for the co-operation and assistance we received from TPS management and staff.

---

[1] INTERPOL-led operation targets growing cyber threats

[2] CBC - RCMP networks targeted by cyberattack

[3] RCMP - Privacy breach affecting current and former employees

[4] The Guardian - Australian federal police officers' details leaked on dark web after law firm hack

[5] BBC - X restricted in Tanzania after police targeted by hackers

## CONTACT

Syed Ali, Assistant Auditor General, IT and Strategy, Auditor General's Office
Tel: (416) 392-8438, E-mail: Syed.Ali@toronto.ca

Andrew Krupowicz, Senior Audit Manager, Auditor General's Office
Tel: (416) 392-3703, E-mail: Andrew.Krupowicz@toronto.ca

Suzanna Chan, Senior Audit Manager (A), Auditor General's Office
Tel: (416) 392-8033, E-mail: Suzanna.Chan@toronto.ca

## SIGNATURE

Tara Anderson
Auditor General

## ATTACHMENT

Confidential Attachment 1: Toronto Police Service IT Infrastructure: Cybersecurity Assessment and Follow-up of Previous Recommendations