

25.



STAFF REPORT ACTION REQUIRED

Cybersecurity Audit of Toronto Public Library

Date: May 25, 2026
To: Toronto Public Library Board
From: City Librarian

Reason for confidential information: *This report involves the security of the property of the Board – Public Libraries Act, R.S.O 1990, Chapter P. 44, s. 16.1 (4) (a).*

SUMMARY

The purpose of this report is to provide a high-level overview of the findings from the Auditor General of Toronto's Report on its cybersecurity audit of Toronto Public Library (TPL).

In early 2025, the Toronto Public Library Board agreed to a request from the Auditor General's office to conduct an independent assessment of TPL's cybersecurity controls. This work was part of the Auditor General's 2025 Work Plan which included a vulnerability assessment and penetration testing of Toronto Public Library's information and technology infrastructure, networks, and systems to assess cybersecurity risks and controls. The audit reviewed selected aspects of TPL's information technology, operational technology, and physical security environments. TPL staff cooperated fully with the Auditor General throughout the audit process and appreciates receiving the feedback and results as an important

component of the continuous enhancement of TPL's information security and accountability.

The Auditor General's detailed findings, recommendations, and management's formal responses are identified in Confidential Attachment 1.

RECOMMENDATIONS

The City Librarian recommends that the Toronto Public Library Board:

1. approve the recommendations in the Auditor General's *Cybersecurity Audit of Toronto Public Library: Overall Assessment of Network, Systems and Physical Security from the Auditor General for information – Report for Action – Attachment 1*;
2. approve the recommendations in Confidential Attachment 1 of the Auditor General's report; and
3. direct that all information contained in Confidential Attachment 1 and Confidential Attachment 2 remain confidential as it involves the security of the property of the Board.

FINANCIAL IMPACT

There is no immediate financial impact associated with this report.

Any future financial implications related to cybersecurity remediation or modernization initiatives will be brought forward through established budget and Board approval processes.

The Director, Finance & Chief Financial Officer has reviewed this financial impact statement and agrees with it.

ALIGNMENT WITH STRATEGIC PLAN

A secure and resilient technology environment is foundational to enabling TPL's Strategic Plan and Digital Strategy. Continued attention to cybersecurity supports reliable service delivery, protects privacy, and maintains public trust in the Library's systems and services.

EQUITY IMPACT STATEMENT

Strengthening cybersecurity controls supports equitable access to library services by helping to ensure that systems remain available, secure, and reliable for all customers and staff, while protecting personal and organizational information.

DECISION HISTORY

At its meeting on April 22, 2025, the Library Board approved TPL's [2025–2029 Digital Strategy](#), which includes objectives for modernized digital services and staff enablement.

ISSUE BACKGROUND

Cybersecurity remains an important area of focus for public sector organizations, particularly those that operate extensive, distributed technology environments and provide broad public access to services and digital resources. TPL operates a complex environment that spans 100 branches, enterprise systems, and public-facing technologies.

The Auditor General's audit provides an independent review intended to assess the effectiveness of existing cybersecurity controls and to identify opportunities to strengthen governance, processes, and risk management practices. The audit complements TPL's ongoing work in enterprise risk management, digital strategy implementation, and infrastructure modernization.

The Auditor General's 2025 Work Plan included a vulnerability assessment and penetration testing of TPL's information and technology infrastructure, networks, and systems to assess cybersecurity risks and controls. The Auditor General's 2025

Work Plan is available at: [Auditor General's Office 2025 Work Plan and Budget Highlights](#)

COMMENTS

TPL management welcomes the Auditor General's audit and views it as an important component of continuous improvement and accountability. Management acknowledges the findings and agrees that there are opportunities to further strengthen TPL's cybersecurity controls and practices.

At a high level, the themes identified through the audit reflect challenges commonly faced by large and decentralized public sector organizations and align with areas already recognized by management as priorities for continued improvement.

These themes include:

- Continued investment in modernizing infrastructure and legacy systems
- Enhancing consistency and standardization of security controls
- Strengthening governance, oversight, and monitoring frameworks
- Ongoing focus on staff awareness, training, and accountability
- Coordinated planning across technology, facilities, and operations

Many of the themes identified through the audit align with work that is already underway or planned, including multi-year modernization initiatives, policy and governance enhancements, and improvements to monitoring and assurance processes. Management will pursue remediation in a prioritized, risk-based manner through established business planning and operations processes.

CONCLUSION

The Auditor General's cybersecurity audit provides valuable independent assurance and insight into TPL's security environment. TPL acknowledges and appreciates the work of the Auditor General's Office and the constructive engagement throughout the audit process.

Management is committed to addressing the identified opportunities for improvement in a deliberate and transparent manner, consistent with TPL's risk management practices, governance framework, and long-term digital strategy.

CONTACT

Steve Till-Rogers, Director, Digital Strategy & Chief Information Officer;
Tel: 416-395-5577; Email: stillrogers@tpl.ca

Alyssa van Graft; Director, Enterprise Projects and Facilities Management;
Tel: 416-395-5541; Email avangraft@tpl.ca

SIGNATURE

Moe Hosseini-Ara
City Librarian

ATTACHMENTS

- Attachment 1: Cybersecurity Audit of Toronto Public Library: Overall Assessment of Network, Systems and Physical Security – Report for Action
- Attachment 2: Confidential Attachment 1: Cybersecurity Audit of Toronto Public Library: Overall Assessment of Network, Systems and Physical Security
- Attachment 3: Confidential Attachment 2: Confidential Presentation to the Toronto Public Library Board



REPORT FOR ACTION WITH CONFIDENTIAL ATTACHMENT

Cybersecurity Audit of Toronto Public Library: Overall Assessment of Network, Systems and Physical Security

Date: May 15, 2026

To: Toronto Public Library Board

From: Auditor General

Wards: All

REASON FOR CONFIDENTIAL INFORMATION

Confidential Attachments 1 and 2 to this report involve the security of the property of the City of Toronto or one of its agencies and corporations.

SUMMARY

The Toronto Public Library (TPL) operates the largest public library system in Canada through TPL's network of 100 branches across Toronto. In 2024, there were 13.4 million in-branch visits and 31.5 million online visits, with approximately 1.1 million registered library cardholders.¹ The TPL's 2025 operating budget was \$269 million, funded mostly by the City of Toronto along with fees, and other revenue sources.²

Technology plays an important role in all aspects of the TPL's operations. This report includes the results of our vulnerability assessment and penetration testing of the TPL's network, systems, applications and devices. We also reviewed user access management, cybersecurity incident logging and monitoring, and tested physical security in relation to cybersecurity.

This report includes three administrative recommendations. The confidential findings and recommendations are contained in **Confidential Attachment 1** to this report. A separate confidential technical report has been provided to management with technical details to guide them in addressing the report findings and recommendations.

¹ TPL 2024 Public Service Statistics, Trends & Comparisons, pages 2, 23 & 32

² Toronto Public Library - 2025 Budget Presentation, page 10

Management agrees with the recommendations in the Confidential Attachment 1, which also includes management's response.

RECOMMENDATIONS

The Auditor General recommends that:

1. The Board receive the public report and Confidential Attachments 1 and 2 from the Auditor General.
2. The Board direct that all information contained in Confidential Attachments 1 and 2 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

Implementing the audit recommendations contained in **Confidential Attachment 1** will further strengthen cybersecurity controls at the Toronto Public Library. 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

The Auditor General's 2025 Work Plan included a vulnerability assessment and penetration testing of Toronto Public Library's information and technology infrastructure, networks, and systems to assess cybersecurity risks and controls. The Auditor General's 2025 Work Plan is available at:

[Auditor General's Office 2025 Work Plan and Budget Highlights](#)

COMMENTS

Cybersecurity threats continue to grow in frequency and sophistication. The Canadian Centre for Cyber Security 2025-2026 National Cyber Threat Assessment report noted that:

"Canada is confronting an expanding and complex cyber threat landscape with a growing cast of malicious and unpredictable state and non-state cyber threat actors...that are targeting our critical infrastructure and endangering our national

*security. These cyber threat actors are evolving their tradecraft, adopting new technologies, and collaborating in an attempt to improve and amplify their malicious activities."*³

Recent Cyberattacks on Public Library Systems

- Toronto Public Library was affected by a cyberattack in October 2023 that disrupted systems and online services across its library branches.⁴
- British Library of the United Kingdom experienced a ransomware attack in October 2023 on its infrastructure affecting systems and data.⁵
- Seattle Public Library was targeted by a ransomware attack in May 2024, disrupting access to staff and public computers, various internal systems, and the library's website.⁶

Since 2015, the Auditor General has proactively audited cybersecurity at the City and has completed several vulnerability assessments and penetration testing of critical systems at the City, and its agencies and corporations. 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.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

The Auditor General will retest cybersecurity controls at the TPL after management has fully implemented the recommendations.

CONTACT

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

Gawah Mark, Audit Director, Auditor General's Office
Tel: (416) 392-8439, E-mail: Gawah.Mark@toronto.ca

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

³ [Canadian Centre for Cyber Security National Cyber Threat Assessment 2025-2026](#)

⁴ <https://www.libraryjournal.com/story/toronto-public-library-recovers-from-ransomware-attack>

⁵ Lessons learned from the ransomware attack on the British library

⁶ Why did ransomware hackers target Seattle public library

SIGNATURE

A handwritten signature in black ink that reads "Tara Anderson". The signature is fluid and cursive, with a long horizontal stroke extending to the right.

Tara Anderson
Auditor General

ATTACHMENTS

Confidential Attachment 1: Cybersecurity Audit of Toronto Public Library: Overall Assessment of Network, Systems and Physical Security

Confidential Attachment 2: Confidential Presentation to the Toronto Public Library Board