TORONTO

REPORT FOR ACTION

Securing Online Confidential Committee and Board Meetings: Sharing Best Practices at the City, and its Agencies and Corporations

Date: January 28, 2025
To: Audit Committee
From: Auditor General
Wards: All

SUMMARY

Over the past five years, the City of Toronto, like many other organizations, accelerated the use of online collaboration and meetings (e.g. using Webex, Teams), in particular due to the Covid-19 pandemic.[1] The use of online meeting platforms continues, owing to factors such as ease of use and hybrid work arrangements.

Hybrid meetings, a combination of in-person and online video conferencing, have become common, including for conducting legislative meetings.[2] This format will stay in use for the foreseeable future. While these meetings have benefits in terms of ease and efficiency, they also introduce cybersecurity and confidentiality risks. It is therefore important to review and further strengthen the practices and controls used in initiating and conducting these meetings, particularly for confidential (in-camera) meetings.

This report highlights the importance for the City to enhance and standardize cybersecurity guidance to City divisions, and to share those best practices with its agencies and corporations for consideration, to proactively prevent unauthorized access to confidential information discussed in these meetings.

Legislative meetings may be closed (in-camera) to the public for specific reasons as outlined in the *City of Toronto Act, 2006*.[3] The City Clerk has developed processes and staff training to secure the electronic portion of closed meetings of City Council, Committees, and local board meetings that are managed by the City Clerk. Similarly,

[1] In July 2020, in response to the Covid-19 pandemic, the Provincial government amended the meeting rules of the *City of Toronto Act, 2006* to allow for electronic participation. In 2023, City Council and most local boards made electronic participation permanent.
[2] Legislative meetings include those held by City Council, Committees and the boards and committees of the City's agencies and corporations
[3] https://www.ontario.ca/laws/statute/06c11 (refer to Section 190)

some agencies and corporations have also developed processes for securing electronic meetings of their boards and committees.

We have noted that while the City has guidelines in place for securing online confidential meetings, these guidelines require further strengthening for cybersecurity considerations, and these need to be distributed across all City divisions, agencies, and corporations for awareness. We have provided examples in this report of observations made by our staff that suggest the need for further strengthening the guidelines.

This report recommends revising the guidelines to be used for online confidential meetings and disseminating them to City divisions, and its agencies and corporations. The critical controls required in initiating and conducting online confidential meetings can also be included in the Chief Information Security Officer (CISO)'s mandatory cybersecurity training.

While the recommended guidance to maintain the security of online confidential meetings in this report relates to meetings of City Council, its committees, and the boards and committees of the City’s agencies and corporations, the CISO can also encourage use of these best practices in the City's internal working meetings where confidential matters are discussed.

The work performed in relation to this report does not constitute an audit conducted in accordance with Generally Accepted Government Auditing Standards (GAGAS). However, we believe we have performed sufficient work and gathered sufficient appropriate evidence to provide for a reasonable basis to support our observations and recommendations.

This public report contains two recommendations to further strengthen and improve controls in initiating and conducting online confidential meetings.

RECOMMENDATIONS

The Auditor General recommends that:

1. City Council request the Chief Information Security Officer, in consultation with the Chief Technology Officer and the City Clerk, to:

    a. Review and revise the existing guidelines to further strengthen best practices and cybersecurity controls for initiating and conducting online confidential meetings for City Council and its committees, and for the consideration of the boards and committees of the City’s agencies and corporations.

    b. Incorporate the critical controls required in initiating and conducting online confidential meetings in the City's annual mandatory Cyber Awareness training.

2. City Council request the City Manager to distribute the Chief Information Security Officer's cybersecurity guidelines for conducting online confidential meetings, to:

a. City divisions, on securing online City meetings where confidential subject matters are discussed, particularly committee and City Council meetings, and

b. City agencies and corporations, including restricted entities, for their consideration to adopt as a best practice for committee and board meetings.

FINANCIAL IMPACT

Implementing the recommendations contained in this report will further strengthen controls in conducting online confidential meetings at the City and its agencies and corporations. The extent of costs and resources needed to implement the recommendation is not determinable at this time. The investment needed to improve controls to manage and respond to cyber threats offsets the potentially significant costs that could result from security breaches.

DECISION HISTORY

The Auditor General recognizes the increased risks presented by cyberattacks and has been proactive in performing cybersecurity assessments and audits at the City since 2016 and plans to continue the important work in this area going forward. The Auditor General's 2025 Work Plan is available at:

https://www.torontoauditor.ca/report/auditor-generals-office-2025-work-plan-and-budget-highlights/

COMMENTS

Since 2020, changes to the *City of Toronto Act, 2006* and Procedure by-law changes have allowed for electronic participation in meetings at the City and its agencies and corporations. While in-person meetings have resumed at the City, hybrid and online options for meetings continue to be leveraged. The City needs to ensure cybersecurity controls and guidelines are in place for initiating and conducting meetings that are closed to the public (in-camera) in accordance with the *City of Toronto Act, 2006*. City agencies and corporations should leverage the expertise, tools, and guidelines of the City's Office of the CISO.

The following observations noted by our staff are provided as examples that suggest improved awareness and uniform cybersecurity guidelines are needed across the City and its agencies and corporations when initiating and conducting online confidential meetings of Council, committees, and the boards and committees of the City's agencies and corporations. The three examples[4] below occurred in meetings where our staff were observing or participating.

- Example # 1: A staff member remained in a confidential meeting for a period of time, although not authorized.
- Example # 2: A staff member was able to log in directly to the confidential meeting due to reused credentials and without authentication.
- Example # 3: Local computer login credentials were communicated over a public session.

Given the importance of security in conducting online confidential meetings, organizations such as the Canadian Centre for Cyber Security[5], US Cyber Security and Infrastructure Security Agency[6], and the National Institute of Standards and Technology[7] have issued various guidelines and bulletins on securing online collaboration and meetings. The City can leverage these guidelines and bulletins to further strengthen its policies and procedures on conducting online confidential collaboration and meetings.

The following are some of the actions that the City should consider when revising the existing guidelines:

- Ensure access to confidential meetings is controlled through appropriate use of unique meeting access codes or passwords. The same passwords or meeting links should not be reused for other meetings or users.

- Enable "waiting room" features as appropriate and use them to ensure the identity of attendees is validated before admission to confidential meetings is granted, with particular care to be followed if a meeting has both public and confidential components.

- Lock online meetings once all intended participants have joined.

- Take appropriate precautions regarding distribution of links to secure meetings and generate unique meeting invitations instead of re-using general purpose

[4] Further details of the City organizations for these examples remain confidential, and have therefore not been included in this report.

[5] https://www.cyber.gc.ca/en/guidance/video-teleconferencing-itsap10216

[6] https://www.cisa.gov/sites/default/files/publications/CISA_Guidance_for_Securing_Video_Conferencing_S508C.pdf

[7] https://csrc.nist.gov/CSRC/media/Presentations/cybersecurity-considerations-for-telework/images-media/5-Greene%20Webinar-slides-06-16-20%20FINAL.pdf

"personal rooms," which are permanently available at the same link. Use the "do not forward" feature when sending a meeting invite where needed.

- Limit or disable meeting recording and file sharing features, as needed.

- Use only City-approved applications for conducting secure online meetings.

We express our appreciation for the assistance we received in finalizing this report from the Office of the CISO, the City Clerk's office, the Chief Technology Officer, and the City Manager's office.

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

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

SIGNATURE

Tara Anderson
Auditor General

ATTACHMENT

Appendix 1: Management's Response to the Auditor General's Report Entitled: "Securing Online Confidential Committee and Board Meetings: Sharing Best Practices at the City, and its Agencies and Corporations"

Appendix 1: Management's Response to the Auditor General's Report Entitled: "Securing Online Confidential Committee and Board Meetings: Sharing Best Practices at the City, and its Agencies and Corporations"

Recommendation 1: City Council request the Chief Information Security Officer, in consultation with the Chief Technology Officer and the City Clerk, to:

a. Review and revise the existing guidelines to further strengthen best practices and cybersecurity controls for initiating and conducting online confidential meetings for City Council and its committees, and for the consideration of the boards and committees of the City's agencies and corporations.

b. Incorporate the critical controls required in initiating and conducting online confidential meetings in the City's annual mandatory Cyber Awareness training.

Management Response: ☒ Agree ☐ Disagree
Comments/Action Plan/Time Frame: The Chief Information Security Officer, the Chief Technology Officer, and the City Clerk agree and support this recommendation. The best practices described within the report are currently available as settings within the City's approved online meeting applications. The meeting host/organizer can apply a combination of these settings depending on the level of confidentiality of their meeting. The Chief Information Security Officer will collaborate with the Chief Technology Officer and the City Clerk to review and update the existing cyber security guidelines according to the best practices described in this report and industry standards by Q1 2025. Additionally, the Chief Information Security Officer will develop a separate training module to address the critical controls required in initiating and conducting confidential online meetings in Q2 2025. From 2026 onward, this separate training module will be amalgamated into the overarching annual mandatory Cyber Awareness Training.

Recommendation 2: City Council request the City Manager to distribute the Chief Information Security Officer's cybersecurity guidelines for conducting online confidential meetings, to:

a. City divisions, on securing online City meetings where confidential subject matters are discussed, particularly committee and City Council meetings, and

b. City agencies and corporations, including restricted entities, for their consideration to adopt as a best practice for committee and board meetings.

Management Response: ☒ **Agree** ☐ **Disagree**

Comments/Action Plan/Time Frame:

The City Manager’s Office agrees and supports this recommendation. The City Manager will ensure the revised guidelines for conducting online meetings are distributed to City divisions, agencies and corporations. It is important that the City, agencies and corporations conduct confidential online meetings effectively and securely.

Revised guidelines will be distributed in Q2 2025 to City divisions, agencies and corporations once they have been finalized by the Chief Information Security Officer, Chief Technology Officer, and City Clerk.