Subject: Office of the Auditor General (OAG) – Audit of Cybersecurity

File Number: ACS2023-OAG-BVG-013

Report to Audit Committee on 27 November 2023

and Council 6 December 2023

Submitted on November 16, 2023 by Nathalie Gougeon, Auditor General

Contact Person: Nathalie Gougeon, Auditor General, Office of the Auditor General (OAG)

613-580-9602, oag@ottawa.ca

Ward: Citywide

Objet : Bureau de la vérificatrice générale (BVG) – Vérification sur la cybersécurité

Numéro de dossier : ACS2023-OAG-BVG-013

Rapport présenté au Comité de la vérification

Rapport soumis le 27 novembre 2023

et au Conseil le 6 décembre 2023

Soumis le 16 novembre 2023 par Nathalie Gougeon, Vérificatrice générale

Personne ressource : Nathalie Gougeon, Vérificatrice générale, Bureau de la vérificatrice générale (BVG)

613-580-9602, bvg@ottawa.ca

Quartier : À l'échelle de la ville

REPORT RECOMMENDATION(S)

That the Audit Committee receive the Audit of Cybersecurity report and recommend that Council consider and approve the recommendations.

RECOMMANDATION(S) DU RAPPORT

Que le Comité de la vérification reçoive le rapport de la Vérification sur la cybersecurité, et recommande au Conseil d'examiner les recommandations, à des fins d'approbation.

BACKGROUND

The Audit of Cybersecurity was included in the 2022-2023 work plan of the Office of the Auditor General (OAG), approved by City Council on December 8, 2021.

A Preliminary Report on Cybersecurity was tabled with Committee and Council in September 2023.

DISCUSSION

In accordance with the Governance report approved by Council on December 7, 2022, the **Audit of Cybersecurity** is being tabled (recommended to be presented *in camera*; see "Legal Implications" section of this report) with the Audit Committee (Document 1).

This report will then be referred to Council for approval of the recommendations.

FINANCIAL IMPLICATIONS

There are no financial implications associated with this report.

LEGAL IMPLICATIONS

There are no legal impediments to the Audit Committee and Council considering this report.

However, the City Clerk and Solicitor, in consultation with the Auditor General, have recommended that the Audit of Cybersecurity be presented to the Committee in closed session and not reported out. The comments set out below explain the underlying rationale for this recommended approach as it relates to the "security of the property" of the City, which is a statutory exemption for a closed meeting.

The open meetings rule, whereby "all meetings" of municipal councils and local boards "shall be open to the public" was enacted in the 2006 amendments to the *Municipal Act, 2001*. In addition, Subsection 239(2)(a) stipulates that a meeting or part of a meeting may be closed to the public if the subject matter being considered is "the security of the

property of the municipality or local board" and this and other exemptions are reiterated in Section 13 of the City's *Procedure By-law*.

As one of the discretionary reasons for a municipal council or local board to consider a matter in camera, it is important to note that the phrase "security of the property of the municipality" has not been expressly defined in the *Municipal Act, 2001*. That said, both the Provincial Ombudsman, who is the Meetings Investigator for over 200 municipalities, and the Local Authorities Services Ltd. (LAS), the Closed Meeting Investigator Program that is available via the Association of Municipalities of Ontario, have issued a number of closed meeting reports that set out the application of this provision. In addition, both of these interpretations are based upon earlier decisions of the Information and Privacy Commissioner of Ontario (IPC). In a 2009 decision involving the City of Toronto, the IPC reviewed the phrase, "security of the property" and concluded as follows:

> In my view, 'security of the property of the municipality' should be interpreted in accordance with its plain meaning, which is the protection of property from physical loss or damage (such as vandalism or theft) and the protection of public safety in relation to the property.

In a further IPC report involving the City of Toronto in 2011, it was determined that the word "property" in the phrase "security of the property" could include both corporeal (having a physical or tangible existence like land) or incorporeal (something that is intangible or not physical, such as a legal right) matters. This analysis has been summarized in the 2013 edition of the LAS document, What You Need to Know About: Closed Meetings in the following manner:

> Property includes not only the physical assets of the municipality but also some of its financial records and intellectual property. Security of information and records, both in hard copy and electronic, are included in this exception.

In addition, the IPC noted that in order to establish that the security of the property exception applies, the municipality must show that it owns the property and that the subject matter being considered at the closed meeting is "security" in the sense of "taking measures to prevent loss or damage to that property". In this same vein, the Ombudsman's Sunshine Law Handbook (3rd edition) states that 'security of the property' includes:

> Discussions relating to the protection of property from physical loss or damage and the protection of public safety in relation to this property.

In light of the above-noted cases and comments, it is suggested that in order for a municipality to rely upon the “security of the property” exemption to hold a closed meeting, it must be able to establish that:

1. It owns the corporeal or incorporeal property identified; and
2. The consideration of the matter at the meeting is, in fact, the security of that property, including taking the appropriate measures to prevent the loss of, or damage to, that property.

I am of the view that the discretionary exception to the open meeting rule for the ‘security of the property’ would meet that two-part test and apply with regards to the Committee considering this report. The property of the City under consideration within the audit includes processes related to IT networks and systems supporting City operations.

COMMENTS BY THE WARD COUNCILLOR(S)

This is a city-wide issue.

CONSULTATION

As this is considered an internal administrative matter, no public consultation was undertaken.

RISK MANAGEMENT IMPLICATIONS

The principles of IT risk management underpin the findings and recommendations outlined within the Audit of Cybersecurity.

SUPPORTING DOCUMENTATION

Document 1 – OAG: Audit of Cybersecurity

Document 1 – BVG: Vérification sur la cybersécurité

DISPOSITION

The OAG will proceed according to the direction of the Audit Committee and Council in considering this report.