SUBJECT: Office of the Auditor General (OAG) – Cybersecurity Investigation Report

File Number ACS2022-OAG-BVG-0004

Report to Audit Committee on 13 June 2022 and Council 22 June 2022

Submitted on June 2, 2022 by Nathalie Gougeon, Auditor General

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

613-580-9602: oag@ottawa.ca

Ward: CITY WIDE / À L'ÉCHELLE DE LA VILLE

OBJET : Bureau de la vérificatrice générale (BVG) – Rapports d'enquête en matière de cybersécurité

Dossier : ACS2022-OAG-BVG-0004

Rapport au Comité de la vérification le 13 juin 2022 et au Conseil le 22 juin 2022

Soumis le 2 juin 2022 par Nathalie Gougeon, Vérificatrice générale

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

613-580-9602; bvg@ottawa.ca

Quartier : CITY WIDE / À L'ÉCHELLE DE LA VILLE

REPORT RECOMMENDATION

That the Audit Committee receive the Cybersecurity Investigation Report and recommend that Council consider and approve the recommendations.

RECOMMANDATION DU RAPPORT

Que le Comité de la vérification reçoive le rapport de d'enquête en matière de cybersécurité, et recommande au Conseil d'examiner les recommandations, à des fins d'approbation.

BACKGROUND

The Cybersecurity Investigation was undertaken as a result of a report made to the Fraud and Waste Hotline.

DISCUSSION

In accordance with the Governance report approved by Council on December 5, 2018, the Cybersecurity Investigation report (recommended to be presented *in camera*; see "Legal Implications" section of this report) is being tabled with the Audit Committee.

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 City Solicitor, in consultation with the Auditor General, have recommended that the Cybersecurity Investigation 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 and "litigation or potential litigation" affecting the City, both of which are statutory exemptions for a closed meeting.

The so-called '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) of those revisions set out a number of discretionary provisions which would enable a municipal council or local board to pass a motion and move into closed session (i.e., in camera) to discuss certain matters, including "labour relations" negotiations or the "proposed or pending acquisition or disposition of land". These same exemptions are reiterated in Section 13 of the City's *Procedure By-law*.

The Cybersecurity Investigation was initiated as a result of a report to the Fraud and Waste Hotline involving cybersecurity risks pertaining to a City-owned asset. The investigation sought to verify the claims made within the report and assess the impact of these risks to the City.

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.

After consulting with the various officers noted above, 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 investigation. The property of the City under consideration within the investigation is a valuable tangible asset. Matters described within the report include technical security controls, which are measures aimed at preventing loss or damage to this property.

Furthermore, it should be noted that the investigation implicates one of the City’s third-party vendors. As such, it may be argued that this portion of the Audit Committee meeting should be held in camera to reduce the risk of litigation against the City.

COMMENTS BY THE WARD COUNCILLOR(S)

This is a city-wide issue.

ADVISORY COMMITTEE(S) COMMENTS

This section does not apply, as this is a city-wide administrative report.

CONSULTATION

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

ACCESSIBILITY IMPACTS

There are no accessibility impacts associated with this report.

RISK MANAGEMENT IMPLICATIONS

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

RURAL IMPLICATIONS

There are no rural implications associated with this report.

TERM OF COUNCIL PRIORITIES

This report supports the Term of Council Priority related to Governance, Planning and Decision Making.

SUPPORTING DOCUMENTATION

There is no supporting documentation associated with this report.

DISPOSITION

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