TORONTO

REPORT FOR ACTION WITH CONFIDENTIAL ATTACHMENT

Non-Competitive Contract for the Provision of Ransomware Resilience Framework & Governance with KPMG LLP

Date: June 22, 2020
To: General Government and Licensing Committee
From: Chief Information Security Officer and Chief Purchasing Officer
Wards: All

REASON FOR CONFIDENTIAL INFORMATION

The attachment to this report involves the security of property belonging to the City of Toronto.

SUMMARY

The purpose of this report is to seek City Council authority for the Chief Information Security Officer to negotiate and enter into a non-competitive agreement with KPMG LLP (KPMG) for professional services for an eight (8) month term. The Services are required immediately to enhance the City's ransomware resilience in order to minimize the impact attackers could cause if they managed to penetrate the City's technology defenses. It is essential to build an effective ransomware resilience framework and governance to enhance the City's capacity to sustain operations and deliver services to its citizens through a cyberattack while minimizing both disruption and reputational harm. Due to time constraints of having these services begin immediately, a competitive call process cannot be done.

The total cost of the agreement with KPMG to build the ransomware resilience framework and governance is $1,978,007 net of Harmonized Sales Tax ($2,012,820, net of Harmonized Sales Tax recoveries).

City Council approval is required in accordance with Municipal Code Chapter 195-Purchasing, where the current request exceeds the Chief Purchasing Official's authority of the cumulative five year commitment for each vendor, under Article 7, Section 195-7.3 (D) of the Purchasing By-Law or exceeds the threshold of $500,000 net of HST

allowed under staff authority as per the Toronto Municipal Code, Chapter 71- Financial Control, Section 71-11A.

RECOMMENDATIONS

The Chief Information Security Officer and the Chief Purchasing Officer recommend that:

1. City Council grant authority to the Chief Information Security Officer to negotiate and enter into a non-competitive agreement with KPMG for a period of an eight (8) month term in the amount of $1,978,007 net of Harmonized Sales Tax ($2,012,820, net of Harmonized Sales Tax recoveries) to develop an effective ransomware resilience framework and governance, on terms and conditions satisfactory to the Chief Information Security Officer and in a form satisfactory to the City Solicitor.

2. City Council direct that the information in the confidential attachment be released when the ransomware risks have been remediated and as the discretion of the Chief Information Security Officer and the City Solicitor.

FINANCIAL IMPACT

The contract has a total value of $1,978,007 net of Harmonized Sales Tax ($2,012,820 net of Harmonized Sales Tax recoveries), and is fixed for the term of the contract.

This will require $1,133,421 net of Harmonized Sales Tax recoveries in 2020 to be implemented. $1,133,421 will be accommodated in the Technology Services Division's Council approved 2020 Capital Budget.

This will also require $879,399 net of Harmonized Sales Tax recoveries in 2021 to be implemented. $879,399 will be requested in the 2021 Operating Budget submissions of the Office of the Chief Information Security Officer.

The funding breakdown by years is included in the following table:

Table 1 –Operating Funding

Division	WBS/Cost Centre	Amount (net of Harmonized Sales Tax recoveries)		
		2020	2021	TOTAL
Technology Services	**CIT046-13-02**	**$1,133,421**		**$1,133,421**

Division	WBS/Cost Centre	Amount (net of Harmonized Sales Tax recoveries)		
		2020	2021	TOTAL
Office of the Chief Information Security Officer	**CY1001**		**$879,399**	**$879,399**
TOTAL		**$1,133,421**	**$879,399**	**$2,012,820**

The Chief Financial Officer and Treasurer has reviewed this report and agrees with the financial impact information.

DECISION HISTORY

There is no decision history.

COMMENTS

Ransomware is now the most prevalent cyber risk to the City as it has become one of the most common cyberattacks on municipalities. Almost one in five cyber incidents is caused by a ransomware attack according to a 2020 Trustwave Global Security Report. Organizations experiencing a cyberattack are having part or all of their environment compromised or cyber criminals are taking possession of the organization's critical data, then leaking it in public forums if the ransomware payment is not made.

A ransomware attack on the City could potentially have negative financial impact, long-term reputational damage, and operational downtime on the City if realized. Even following a complete recovery and resumption of services, the City could incur expenses resulting from regulatory fines, forensics investigations, legal fees due to legal actions taken against the City, and rebranding campaigns due to the erosion of public trust and confidence.

Cyber security risk is real and pervasive, as seen in recent ransomware attacks on other municipalities. Building the City's ransomware resilience is critical to enable the City to adequately respond to and recover from effectively to a ransomware attack.

KPMG's cyber security advisory team has extensive experience servicing federal and municipal clients in Canada and Globally. KPMG has an intimate knowledge of the City’s cyber posture from the comprehensive cyber maturity assessment they conducted in 2018-2019 during which KPMG's team spent many months learning about the City’s environment.

In December 2019, KPMG performed a ransomware assessment for the City and thirteen (13) of its Divisions with IT units. They have a deep understanding of the current state of the City's cyber posture, they will prioritize the work efforts accordingly, and can hit the ground running with the steps necessary to enhance the cyber governance controls as they have the necessary foundational knowledge. This knowledge and speed of delivery will assist the City in recouping the time lost during COVID-19 as priorities understandable focused on recovery.

With the knowledge KPMG has gained of the City's digital infrastructure and cyber posture, and under the City's direction, utilizing them to help provide the cyber governance controls and mitigate identified risks allows the City to improve its' cyber resilience on an accelerated timeline with substantial cost avoidance.

A substantial discount for the professional services has also been offered to the City considering the City's financial circumstances due to COVID-19. Leveraging existing relationships with cyber security product vendors, KPMG has been able to provide complete and accurate licensing and solution requirements along with competitive pricing aligned with City's financial requirements.

Additional information details on the non-competitive contract is outlined in the confidential attachment #1.

The Fair Wage Office has reported that KPMG LLP has indicated that it has reviewed and understands the Fair Wage Policy and Labour Trades requirements and has agreed to comply fully.

CONTACT

Eric Lawton, Office of the Chief Information Security Officer
Tel: (416) 397-4334, Email: Eric.Lawton@toronto.ca

Jacquie Breen, Manager, Corporate Purchasing Policy & Quality Assurance
Purchasing and Materials Management Division
Tel: 416-392-0387, Email: Jacquie.Breen@toronto.ca

SIGNATURE

_____

Kush M. Sharma
Chief Information Security Officer

_____

Michael Pacholok
Chief Purchasing Officer

ATTACHMENTS

Confidential Attachment 1 - Ransomware Resilience Framework & Governance