For Action
with Confidential Attachment

Contract Award for Managed Security Services

Date: July 14, 2022
To: TTC Board
From: Chief Financial Officer

Reason for Confidential Information

This report contains information related to the security of the property of the municipality or local board.

Summary

The purpose of this report is to obtain TTC Board authority to award the contract for the provision of Managed Security Services and other associated information security services in the amount of $28,165,777.50, inclusive of Harmonized Sales Tax (HST), for a duration of up to six years on the basis of highest-ranking proposal score. The contract includes the option to extend the term of the contract for two individual, two-year terms to be exercised at the TTC's sole discretion. The contract is targeted to start August/September 2022.

This award consists of:

1. One-time capital costs: $4.90 million plus HST, which enables the procurement of tools (hardware/software), the provision of implementation services that include planning, system design, testing and the implementation all security solutions within the scope of the contract; and
2. Ongoing operating costs: $20.7 million plus HST, which provides the TTC the support, maintenance and enhancement of the deployed security solutions.

Procuring managed security services is key to the TTC's intent to continuously strengthen the security posture of an integrated Information Technology (IT) and Operational Technology (OT) critical infrastructure organization, such as the TTC. Faced with unique cybersecurity challenges, unprecedented pace and increased complexity of cyber attacks, coupled with a shortage of cybersecurity professionals, the need for a holistic security solution that addresses all means of cyber threats is crucial to enabling the TTC to deliver its services.

The objectives of this contract are to:

- Reduce the TTC's enterprise risk, while enhancing the TTC's overall security posture in a manner that supports demonstrable cybersecurity compliance and regulatory compliance.

- Access 24-hour, year-round security coverage, which includes access to supplier expert resources as needed in the case of remote incident response.
- Provide a comprehensive and scalable solution for managing security, performance and compliance resulting in a robust, reliable security environment for the TTC.
- Accelerate threat detection and response capabilities while providing greater control and visibility of the security and functionality of the TTC's environments, networks and other IT assets.
- Integrate and inter-operate with the TTC security team and security governance by providing analyzed, prioritized and actionable information and outcomes.
- Provide ongoing knowledge transfer to the TTC security team as required for the TTC to fulfil its obligations in respect of the services over time and accounting for any new technology that will be deployed.

The scope of work of this contract will be delivered by the Managed Security Services (MSS) Provider identified as providing the best solution and value to the TTC through the evaluation process set out in the Request for Proposal (RFP). The scope includes, but is not limited to, the system design, implementation, support and management of the following listed core security solutions for both the IT and OT environments:

1. **Managed Detection and Response (MDR)**: Security tools and services to detect malicious network activity and respond to eliminate the threat quickly;
2. **Security Operations Centre (SOC)**: A centralized security function that will be implemented and managed by the vendor to proactively monitor network activities 24 hours per day, year-round, to improve the overall security posture of the TTC; and
3. **Security Solutions and Services (SSS)**: Essential security services to keep the TTC network safe from known security threats that could be exploited by attackers as well as aid regulatory compliance.

The contract also contains provisions to enhance the services provided to keep pace with evolving cybersecurity solutions and to provide knowledge transfer services to advance the TTC's maturity of its cyber team as well as staff augmentation services to add resources to the team, as may be required.

The TTC Cybersecurity Program is a fundamental initiative to achieving all five critical paths identified in TTC's Five-Year Corporate Plan 2018-2022. This program is focused on implementing various security initiatives identified in the Cyber Program to mitigate cybersecurity risks.

Recommendations

It is recommended that the TTC Board:

1. Authorize the award of contract for the provision of Managed Security Services and other associated security services to IBM Canada Ltd. for an initial term of five years, in the amount of $28,165,777.50, inclusive of HST, with two, two-year extensions, to be exercised at the TTC's sole discretion.

Financial Summary

The contract award value consists of capital costs of $4.90 million and operating costs of $20.5 million, after accounting for the HST rebate.

The capital costs to be incurred as part of this contract will provide the necessary hardware, software license, software subscriptions and vendor professional services required for the implementation of cyber tools. Capital software subscription license costs are for software subscriptions used during the project implementation phase required in the delivery of the cybersecurity solution.

Funding for the capital costs of $4.90 million (including HST) for this contract award are included in the TTC's 2022-2031 Capital Budget and Plan, as approved by the TTC Board on December 21, 2021 and by City Council on February 17, 2022 under Program 7.20 Information Technology Services, Cybersecurity Project.

The total project budget for the Cybersecurity Project is $14.18 million comprising of costs to the end of 2021 of $3.47 million and funding of $10.71 million cashflowed between 2022 and 2025. Of the approved funding in the 2022-2031 Capital Budget and plan, approximately $2.22 million has been committed to date.

Operating costs to be incurred reflect the service costs that will be paid annually for managed services, software maintenance, support and software subscription licenses. As shown in Table 1 below, a total of $3.08 million is required in 2023 for costs under this contract, with a total requirement of $20.47 million over the term of the contract.

The total operating funding requirement for 2023 is $3.83 million, which includes the operating cost of the MSS contract and operating costs for interim cybersecurity services. The 2022 Operating Budget includes $1.78 million for current Managed Security Services, which can be used to partially offset and thereby reduce the incremental 2023 funding requirement to $2.05 million. The remaining $2.05 million will be submitted in the TTC's 2023 Operating Budget submission and corresponding amounts for future operating budgets based on each year's anticipated spending requirements.

Table 1 below outlines the capital and operating expenditures for each year of the contract term for the services provided by this contract.

Table 1: Contract Cost Summary ($ in millions)

Cost Description	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	**2028**	**Total**
Capital Costs								
Managed Detection and Response	0.17	0.52						
Security Operations Centre	0.94	0.91						
Security Services Solutions	0.39	1.97						
Subtotal Capital Costs	*1.50*	*3.40*						**4.90**
Operating Costs								
Managed Detection and Response		0.75	0.96	0.98	0.99	1.02	0.32	
Security Operations Centre		1.20	1.35	1.36	1.36	1.33	0.54	
Security Services Solutions		1.12	1.61	1.62	1.63	1.64	0.70	
Subtotal Operating Costs		3.08	3.92	3.95	3.98	3.98	1.56	**20.47**
Recoverable HST	0.17	0.72	0.43	0.44	0.44	0.44	0.17	**2.80**
Total	**1.66**	**7.19**	**4.35**	**4.39**	**4.42**	**4.42**	**1.73**	**28.17**

While there are two optional two-year extensions (total four years) available to be exercised for this MSS contract, the TTC will reassess its business requirements, market conditions and options available at that time before any extension is executed to ensure a cost-effective price is achieved.

Equity/Accessibility Matters

A cornerstone of TTC’s Corporate Plan 2018-2022 is accessibility and being a proud leader in providing accessible public transit in the city of Toronto. We are committed to ensuring reliable, safe, accessible and inclusive transit services for all our customers. This is supported through the continued work of the TTC Cybersecurity Program and the implementation of its various security initiatives.

The services acquired through the MSS contract further strengthen cybersecurity capabilities to protect the confidentiality of employee and customer data. Additionally, it ensures the integrity and availability of the TTC’s transit services.

Decision History

At the December 13, 2017 meeting of the Audit and Risk Management Committee, staff presented a presentation entitled, Presentation: Cyber Security Risks and Mitigation Strategies – Information Technology Services which provided the Committee with an understanding of key cybersecurity risks and mitigation strategies associated with the TTC's systems.

In October 2019, City Council adopted the recommendations in the Cyber Safety: A Robust Cybersecurity Program Needed to Mitigate Current and Emerging Threats report. As a result, City Council:

1. Requested all Agencies, Boards and Commissions (ABCs) to provide a cybersecurity enterprise risk assessment by the third quarter of 2020, to the City's Chief Technology Officer (CTO).
2. Directed the City's CTO:
    a. To provide support, oversight and directions on standards, practices and policies to all ABCs;
    b. To work with the ABCs to assess regulatory and compliance matters and their impact on moving to a centralized information technology service; and
    c. To report on an implementation plan for a centralized model to provide oversight and approval for all technology assets, goods and services purchased by ABCs, including the TTC.

On December 12, 2019, the TTC Board adopted Recommendation 1 of City Council's decision, and supported, in principle Recommendation 2 to provide the necessary support to the City's Chief Technology Officer, in order to respond to City Council's direction.
Decision: City Council Transmittal – Audit Committee Item 4.1 – Cyber Safety: A Robust Cybersecurity Program Needed to Mitigate Current and Emerging Threats

At its meeting on June 17, 2020, the TTC Board considered a report entitled, TTC Status Update – Information and Cybersecurity Strategy and adopted staff recommendation to endorse the Information and Cybersecurity Strategy that was outlined in the report.

Issue Background

The TTC, a critical infrastructure organization, has a requirement for high availability for service delivery, coupled with the magnitude of impact from potential risks to public safety, security and financial implications of service disruptions. This makes it an attractive target for cyberattacks, as recently witnessed in October 2021.

Increased risks to the TTC can be attributed to the growth in attack vectors across the Internet, the increased sophistication of malicious actors, and the changing global political and technological landscape.

Additionally, the convergence of corporate and industrial systems to enable a modern-day transit-based technology infrastructure increases the risk and exposure to cyber threats, thus making various mission- and safety-critical systems vulnerable to attacks.

To mitigate and defend against these threats, the TTC developed an information and cybersecurity strategy and established a program to implement various security initiatives.

Information and Cybersecurity Strategy

The TTC’s strategy for information and cybersecurity has four strategic pillars built upon the core functions (i.e. Identify, Protect, Detect, Respond and Recover) within the National Institute of Standards and Technology (NIST) framework for Improving Critical Infrastructure Security. They are:

1. Mature governance and risk management practice;
2. Strengthen cybersecurity capabilities to enable safe and secure transit operations;
3. Improve cybersecurity resiliency in detecting, responding and recovering from incident and breaches; and
4. Advance overall standing on cybersecurity posture.

The action plan for this strategy is the Cybersecurity Program. This program leverages findings from third-party Security Assessments as well as recommendations from peer reviews (American Public Transportation Association and International Association of Public Transport) to build the TTC’s risk-based approach in managing cybersecurity.

In accordance with the Information and Cybersecurity Strategy’s pillars 3 and 4, the TTC issued a structured Request for Proposal (RFP) for implementation of a comprehensive Managed Security Services (MSS) and associated Security Services for both the TTC’s IT and OT environments. Given the MSS is a very complex solution, comprising multiple components, the structured RFP was leveraged to select products and services to achieve maximum protection within the available budget.

Managed Security Services and Associated Security Services

The current complex and targeted cyber threat landscape requires around-the-clock monitoring that involves a significant investment in both technology tools, infrastructure upgrades/replacements and the on-boarding of an extensive specialized cybersecurity workforce.

Managed Security Services is considered the best cybersecurity defense as the vendor partners with the TTC to implement security solutions as well as provide 24-hour, daily security monitoring and management. The MSS, in addition to augmenting staff and advancing the maturity of TTC cybersecurity staff teams, will work with the TTC to implement solutions that will improve the TTC’s enterprise security capabilities.

The key benefits for the provision of MSS are summarized below:

- Strengthened cybersecurity posture with 24-hour, daily monitoring and threat detection, proactive threat hunting, vulnerability and patch management;
- Dedicated support and faster access to unique security expertise and intelligence;
- Reduced regulatory risks provided through automated compliance;
- Solution is highly scalable and adaptable to changing business needs; and
- Knowledge transfers to advance maturity of internal Security teams.

Comments

RFP Scope Development

In developing the scope for this RFP, the TTC leveraged information from the following sources, which were validated with Gartner research reports:

- Findings from third-party, vendor-conducted security assessments of the TTC's IT and OT environments to incorporate recommendations and insights;
- Security frameworks and standards, such as those from the Center for Internet Security (CIS) critical security control benchmarks and the National Institute of Standard and Technology (NIST) framework for improving critical infrastructure to ensure alignment;
- Adopted recommendations from the Cybersecurity and Infrastructure Security Agency (CISA) on securing critical infrastructure;
- Recommendations from peer reviews conducted with the American Public Transportation Association (APTA) and the International Association of Public Transport (UITP) in Europe; and
- Findings from Gartner reviews and workshops to drive maturity assessment, identify security gaps and the roadmap to address.

Multi-phase RFP process

The nature of the TTC's IT and OT integrated environments requires a holistic approach on implementing state-of-the-art security controls and solutions through a single accountable MSS provider rather than disparate technologies providers. To ensure that a knowledgeable solution provider with proven experience and mature solution offerings was selected, the TTC conducted a multi-phase RFP.

Phase 1 RFPQ:
The TTC leveraged Gartner Magic Quadrant and Forrester Wave reports to identify a list of 68 vendors for a publicly advertised Request for Pre-Qualification (RFPQ) (Reference #: P25PZ21201) posted on MERX on June 1, 2021. Twelve vendors responded by the closing date of July 5, 2021 and after the evaluation process, eight out of 12 were pre-qualified and invited to Phase 2 of the rigorous procurement process.

Phase 2 RFP:
To ensure a successful process that is aligned with industry best practices, the TTC retained the services of a third-party procurement consulting firm to provide support to

the Procurement and Category Management (PCM) Department in the development and preparation of the procurement documents. The RFP was issued on November 1, 2021 to all pre-qualified vendors with an initial submission deadline of December 30, 2021, which was extended to January 12, 2022 based on vendor requests for an extension. Seven vendors submitted proposals by the submission date of January 12, 2022.

Evaluation of the Proposal Submissions

The seven proposals received were reviewed for commercial compliancy and they were all confirmed to be compliant, hence all proposals were rated by the evaluation team.

A fairness monitor was retained by the TTC to ensure that the procurement process took place in accordance with the requirements established in the RFP and to ensure fairness and transparency during this process. The Fairness Monitor’s report, attached as Appendix 3, confirms the fairness of the process based on their observations.

The PCM Department conducted training for all four members of the evaluation team from the Information Technology Services Department together with the Fairness Monitor in attendance, to best understand the overall RFP process consisting of seven unique stages, the expectations for the evaluator role and the required commitment to meet the procurement schedule. Evaluators conducted the formal review and rating in accordance with the requirements outlined in the RFP. An employee from the PCM Department acted as the facilitator during the evaluation process.

The recommendation for award is based on the highest scoring proponent. The evaluation of proposals was based on a qualitative, demonstration and price component; 60.00 points allocated to the qualitative merit; 11.00 points allocated to the demonstration; and 29.00 points allocated to pricing. Proposals were first scored based on qualitative criteria at the associated weightings set out in the RFP documents.

A minimum threshold was set for five key evaluation criteria, namely: Solution Description, Rated Requirements, Evaluation Scenarios, Implementation Services and Professional Services. Proponents who passed the minimum threshold and received at least 44.592 out of 74.32 points (60%) in Stage II would be considered qualified to proceed to the next stage. Proponents scoring below the threshold were eliminated from the evaluation stage and not evaluated further.

The minimum threshold for the demonstration stage was 9.1 out of 14 points (65%). One proponent met this threshold and advanced to the pricing evaluation stage. The pricing component for the proponent was then evaluated. The total weighted score was calculated as a sum of the weighted qualitative score and the weighted pricing score.

IBM Canada Ltd. received the highest total weighted score and is recommended for award of the contract.

Contact

Dhaksayan Shanmuganayagam, Head – Information Technology Services
416-393-3922
dhaksayan.shanmuganayagam@ttc.ca

Signature

Josie La Vita
Chief Financial Officer

Attachments

Confidential Attachment 1 – Managed Security Services and Cybersecurity Update
Confidential Attachment 2 – RFP P25PZ21558 Recommendation Report
Appendix A – Fairness Monitor's Report

Request for Proposals (RFP #P25PZ21558)

Managed Security Services

Toronto Transit Commission

Final Fairness Report

Project:	TTC RFP P25PZ21558
Report Stage:	Request for Proposal (RFP) Final Fairness Report
Date of Submission:	July 5, 2022
Submitted to:	Director of Procurement

TABLE OF CONTENTS

1 INTRODUCTION

BDO Canada LLP (BDO) was engaged by the Toronto Transit Commission (TTC) as a Fairness Monitor to observe the Request for Proposals (RFP #P25PZ21558) process of the Managed Security Services RFP.

BDO's engagement on this project started on August 31, 2021, following the issuance of the purchase order for the provision of Fairness Monitor Services. We were not involved in this project prior to award of the call-up.

BDO will be the Fairness Monitor for the Managed Security Services RFP.

We hereby submit this Final Fairness Report for the Request for Proposal (RFP) report covering the activities and monitored observations of the Fairness Monitor for RFP #P25PZ21558 Managed Security Services RFP.

BDO is an independent third party with respect to this activity. We reviewed all the information provided and observed all relevant activities as described below and in accordance with our mandate.

This report includes our attestation of assurance, background of the project, a summary of the scope and objectives of our assignment, the RFP process, RFP evaluation process and relevant observations from the activities undertaken.

2 ATTESTATION OF ASSURANCE

It is our professional opinion that the Managed Security Services Request for Proposal (RFP #P25PZ21558) RFP Posting to RFP Close activities and process that we observed, was carried out in a fair, open and transparent manner.

DocuSigned by:
Kelly Campbell
E7DA09D0E1E9413...

Ian Brennan
Fairness Monitor

Kelly Campbell
Partner

3 PROJECT BACKGROUND

As part of its overall cyber security strategy, the TTC requires a cyber security service provider that offers hosted Managed Detection and Response (MDR), Managed Security Services (MSS), Professional Services (Security) and other related security services to work with the TTC staff to secure the TTC Information Technology (IT) and Operational Technology (OT) environments. The solution is expected to be an industry recognized turnkey MSS and MDR offering that is proven in the market, reliable, resilient, cost effective, flexible and owned and operated by a mature and stable corporation.

In order to strengthen TTC's Security posture, TTC Information and Technology Services Department is embarking on a comprehensive Cybersecurity program to address the growing concern of cyberattacks. With the unprecedented pace and complexity of cyberattacks, its transit system must be proactive and adopt a holistic approach to securing TTC's information infrastructure.

Being in the public sector, TTC must observe legislative, regulatory, political and socioeconomic drivers in planning and executing its strategic corporate objectives, including its approach to enterprise Information Security and Risk Management. Compounding the challenges to meet traditional mandated Information Security (IS) requirements while supporting a mass ridership across the GTA, TTC is faced with specialized IS threats affecting critical Transit infrastructure.

The high availability requirement for TTC service delivery, coupled with the magnitude of potential risks to public safety, security and financial implications of service disruptions, makes TTC an attractive target for cyber-attacks. Increased risks to TTC can be attributed to the proliferation of the cyber threat vector across the Internet, the increased sophistication of bad actors, and the changing global technological landscape.

Accordingly, TTC requires Proposals for a comprehensive Managed Security Service ("MSS") solution and associated services ("Solution") that contemplates securing all aspects of TTC's information technology ("IT") and OT environments in accordance with the Deliverables described below. TTC is looking for Proponents to apply their security platforms augmented with such other tools, information or capabilities as is necessary to meet the Deliverables.

4 FM ENGAGEMENT AND OBSERVATIONS

BDO Canada LLP (BDO) was engaged by TTC as a Fairness Monitor to observe the Request for Proposals (RFP #P25PZ21558) to oversee the procurement process in accordance with the pre-established guidelines as set out in the RFP and to ensure the fairness and transparency during the procurement process. This includes but is not limited to request for proposal (non-binding), evaluation, negotiation, contract award, and proponent debriefing (optional, as required).

As per our scope of services and following Notification of Award, the TTC will provide the Fairness Monitor with a copy of the RFP document, evaluation forms, addenda issued, and any information relevant to the procurement process.

The Fairness Monitor shall not provide comments on whether the correct proponent has been selected, but rather to ensure that TTC's internal evaluation process is being followed and that all proponents are treated fairly and equally.

In accordance with the terms of our engagement, we familiarized ourselves with the relevant draft and final documents, observed activities up to the end of the RFP stage and subsequent proposal evaluation stage. We identified fairness-related matters to the RFP project team and ensured that responses and actions were reasonable and appropriate procurement process and to attest to the fairness, openness and transparency of this monitored activity.

As Fairness Monitor, BDO's mandate is to act as an independent third party to monitor and ensure the integrity of the procurement process, indicating whether the process was managed fairly, consistently, openly, competitively and transparently.

In order to do so, and in accordance with our scope of services and responsibilities, BDO:

1. Review and understand the TTC's procurement by-laws, policies, processes, and procedures;
2. Become familiar with the RFP document as issued and the evaluation process;
3. Review various documents and information, including but not limited to the procurement documents, addendum, and correspondence
4. Review the evaluation criteria with respect to clarity and consistency;
5. Identify situations and issues which may compromise the evaluation process, and which may result in complaints about the procurement process and provide advice on resolving complaints;
6. Provide oversight and advice during the procurement process;
7. Attend Pre-Bid Meetings;
8. Review each Bid submission;
9. Attend Commercial and Technical Evaluation Meetings;
10. Participate in telephone calls with TTC's Legal and/or Procurement and Category Management Departments;
11. Ensure that all participants were briefed on best practices with respect to principles and duties of fairness; confidentiality of vendor submissions; conflict of interest; undue influence; scoring procedures; and the retention of documents;
12. Upon completion of the evaluation process, prepare a report describing the Fairness Monitor's observations and findings throughout the process;

13. Attend the TTC's Board Report Meeting to answer questions regarding the report or process, if called upon to do so;
14. Attend Debriefing meetings (if required) and provide comments on the fairness of the selection process.

4.1 RFP DEVELOPMENT AND RFP SUPPORTING DOCUMENTS

The TTC acquired the service of an external procurement consultant (GEF Consulting) to lead the development of a negotiated Request for Proposal (nRFP). The TTC along with GEF Consulting were seeking and RFP format that would allow reasonable flexibility during the nRFP to ensure the needs of the TTC were met and allow for industry feedback within the confines of the nRFP process. This included having Commercial Confidential Meetings (CCM's) and a Best and Final Offer (BAFO); Proof of Solution (PoS) within the RFP process.

The nRFP Scope of Services and technical specifications were developed by TTC's ITS (Information Technology Service) department.

BDO was not involved in the development of the RFP or RFP supporting documents.

The TTC RFP project team provided the RFP documents to BDO. BDO conducted a review of the following documents:

- RFP Body
- Appendix A Scope
- Appendix B – Form of Agreement – (Not reviewed by BDO)
- Appendix C – TTC Organizational Overview
- Appendix D – Demonstration Process and Instructions
- Appendix E – Company Submission Form
- Appendix F Mandatory Technical Requirements
- Appendix G – Proposed Solution Submission
- Appendix H – Pricing Submission Form
- Appendix I - Form of Agreement Review Submission Form

4.2 RFP Process Timetable

As per Section 1.5, RFP Timetable, provided the key RFP dates to the proponents. All revisions to dates were through Addendums issues by TTC. Below is the timetable of events for the RFP:

Step in the Procurement Process	Date
Issuance of RFP	**November 1, 2021**
Proponent Briefing Posted Video	**November 10, 2021**

Step in the Procurement Process	Date
Deadline for Questions	**December 10, 2021**
Deadline for Responding to Questions	**December 15, 2021**
Deadline for Issuing Addenda	**January 3, 2022**
Submission Deadline #1 Written Proposal (All Proponents)	**January 12, 2022**
Rectification Period	**3 business days**
Submission Deadline 2 Recorder Demonstration Scenarios (Shortlisted Proponents Only)	**February 22, 2022**
Anticipated Commercially Confidential Meetings (CCM's)	**March 14 -16, 2022**
Anticipated Best and Final Offer (BAFO) Submission deadline	**April 5, 2022**

5 RFP PHASE 1 OPEN PERIOD

5.1 RFP Phase 1 Open Period

The RFP Open Period began when TTC issued RFP Managed Security Service #P25PZ21558 on November 1, 2021. The RFP was issued on Bonfire.

5.2 Proponents Briefing Video

As per the RFP section 1.5.2, TTC provided for a Proponents RFP Briefing Video on November 10, 2021.

TTC posted one (1) pre-recorded Proponent briefing video. All interested Proponents were encouraged to download and review the briefing video. TTC advised that attendance at the Proponents Briefing Video was not mandatory and that there were no consequences in the evaluation process for not attending the Proponents Briefing Video.

The briefing video covered a high-level overview of the RFP process, including submission requirements, timelines, and scope. Following review of the briefing video, Proponents are encouraged to submit all technical questions in writing in accordance with Section 3.2 – Communication after Issuance of RFP. Any additional material will be made available to Proponents in accordance with Section 3.2.3 – All New Information to Proponents by Way of Addenda.

5.3 Request for Information

Proponents were encouraged to submit questions to the contact person identified in the RFP.

As per the RFP, Proponents submitted all questions electronically thru Bonfire to the contact person in accordance with the instructions set out in the RFP.

TTC received 239 questions from Proponents during the RFP open period. TTC RFP project team was very diligent in addressing all the questions received from the Proponents. TTC responded to all 239 questions. Before issuing the responses to the Proponents questions, the responses were sent to the Fairness Monitor to review. The TTC project team addressed all comments raised by the Fairness Monitor.

As per the RFP timelines, the Proponents last day to submit questions was December 10, 2022. TTC's last day to post responses to a Proponent's questions was December 1, 2021.

The process to address Proponents questions conducted by TTC conformed to the process defined in the RFP.

5.4 RFP Addendum

TTC issued two (2) Addenda during the RFP process. All Addenda were uploaded to Bonfire. Per the RFP, the last day for issuance of Addenda by TTC was January 3, 2022.

The RFP Addendum process conducted by the TTC conformed to the process defined in the RFP.

5.5 RFP Written Proposals Submission Deadline

As per RFP section 1.6 Submission of Proposal the submission deadline was December 8, 2021 (no later than 4:00:00 pm. Local time). TTC received seven (7) submission before the submission deadline.

RFP Posting to Close Summary

The RFP Posting to RFP Close activities and processes defined in the RFP were adhered to by the TTC RFP project team. RFP Posting to RFP Close activities and processes that we observed were fairly and consistently applied and in accordance with the RFP. All Proponents were treated fairly, and all proponent questions were addressed in accordance with the criteria in the RFP. We detected no bias or favouritism towards any Proponent.

6 EVALUATION OF SUBMISSIONS

6.1 RFP Evaluation Committee Training

The Evaluator Committee Training session was held on January 18, 2022. The purpose of the meeting was to review the objectives of the evaluation process, the evaluation framework and process documents, the participant structure, roles and responsibilities, the evaluation and scoring, the evaluation tools, procedures and considerations, and to discuss evaluator confidentiality and disclosure of any perceived, potential or actual conflicts of interest.

The Fairness Monitor was present for the evaluator training presentation. No conflicts of interest were declared by the participants during the evaluator training presentation.

6.2 Evaluation Process

As per section 2.1 of the RFP, the TCC outlined the evaluation of the proposals and negotiations in the following stages. TTC received seven (7) submissions from the following companies

- Accenture
- Deloitte
- IBM Canada Limited
- In Fidem
- SourectekIT
- Stratejm Inc.
- Tata Consultancy Services Canada Inc.

6.3 Stage I - Mandatory Submission Requirements

As per section 2.2 of the RFP, Stage 1 Mandatory Submission requirements consisted of the following two substages.

6.3.1 Mandatory Form Requirements

As per section 2.2.1 of the RFP, Stage I will consist of a review to determine which Proposals comply with the mandatory form requirements.

The Evaluation committee team reviewed each proponent's mandatory form requirements and the contents of the form to assess its compliance with the terms and conditions of the RFP documents. For proposals where the Evaluation committee had identified deficiencies, the TTC issued the Proponent a rectification notice identifying the deficiencies and providing the Proponent an opportunity to rectify the deficiencies.

The process to review mandatory form requirements conducted by the evaluation committee conformed to the process defined in the RFP.

6.3.2 Mandatory Technical Requirements

As per section 2.2.2 of the RFP, Stage I will consist of a review to determine which Proposals comply with the mandatory technical requirements.

The Evaluation committee team reviewed each proponent's mandatory technical requirements and assess its compliance with the requirements as set out in Part 4 - RFP Particulars, section D Mandatory Technical Requirements have been met.

Where the Evaluation committee identified questions or queries as to whether a Proposal has met the mandatory technical requirements, those proposals will be subject to the verification and clarification process set out in Section 3.2.4 (Part 3). Proposals that do not demonstrate compliance with these mandatory technical requirements will be excluded from further consideration.

The process to review mandatory technical requirements conducted by evaluation committee conformed to the process defined in the RFP.

6.3.3 Rectification Period

As per section 2.2.3 of the RFP, if the Stage I requirements are not satisfied, the Proponent will be notified and will be given the amount of time as stated in the Section 1.5 RFP Timetable to rectify. The Rectification Notice will state the date and time that the rectification notice response is due. The TTC did issued Rectification Notices to the Proponents.

The process for rectifications conducted by the evaluation committee conformed to the process defined in the RFP.

All seven (7) submissions passed the Mandatory Submission requirements and move forward to Stage II Rated Criteria.

6.4 Stage II - Rated Criteria

TTC evaluated each qualified proposal on the basis of the non-price rated criteria as set out in Section E of the RFP Particulars (Part 4).

Proponents were required to meet a minimum threshold of 60% in Stage II in order to be eligible to participate in subsequent stages in the evaluation process. TTC reserved the right, in their sole discretion, to waive this Stage II minimum threshold in the event that none of the Proponents met the minimum threshold, and instead, will allow the four (4) highest scoring Proponents from Stage II to participate in subsequent stages in the evaluation process.

Two proposals were successful in Stage II and satisfied the minimum threshold of 65% in order to be eligible to participate and move forward to Stage III. The Proponents moving on to Stage III are Accenture and IBM.

The process to review rated criteria requirements conducted by the evaluation committee conformed to the process defined in the RFP.

6.5 Stage III – Recorded Demonstration Scenarios

As per section 2.4 of the RFP, the TTC shortlisted two top-ranked Proponents based on the accumulated scores at Stage II. These shortlisted Proponents were invited to submit recorded demonstrations of the capabilities of their Proposed Solutions. Notices were sent to both

Accenture and IBM on February 16, 2022 to notify them that they had been successful in moving forward to Stage III and that they were requested to submit their Recorded Demonstration Scenarios by February 25, 2022 (12:00pm local time).

The Recorded Demonstration Scenarios submitted by the Proponents were required to accurately represent the Proposed Solution described in the Proposal, without introducing any changes or additional out of scope materials. Proponents were to only demonstrate functionality that has been included in their Proposal.

Proponents were required to meet a minimum of 65% in Stage III in order to be eligible to participate in subsequent stages in the evaluation process. TTC, reserved the right, in their sole discretion, to waive this Stage III minimum threshold in the event that none of the Proponents can meet the minimum threshold.

One proposal was successful in Stage II and satisfied the minimum threshold of 65% in order to be eligible to participate and move forward to Stage IV. The Proponent moving on to Stage IV was IBM.

The process for Recorded Demonstrations Scenarios conducted by the evaluation committee conformed to the process defined in the RFP.

6.6 Stage IV – Pricing and Form of Agreement

As per section 2.5 of the RFP, Stage IV the Pricing Submission Form (Appendix H) and the Form of Agreement Review Submission Form (Appendix I) will be opened in Stage IV. This stage will be undertaken after the evaluation of mandatory requirements and rated criteria has been completed. For clarity, pricing will not be scored during Stage IV.

6.7 STAGE V Commercially Confidential Meetings (CCM's)

As per section 2.6 of the RFP, State V will consist of CCM's with the shortlisted Proponent and the TTC. There is no evaluation component to the CCM. The CCMs will allow for meaningful dialogue regarding the shortlisted Proponent proposal. In addition, TTC anticipates providing the shortlisted Proponents with the opportunity to seek clarification regarding specifics of TTC's environment which may allow for clarity on how Proponents are to price their Proposal.

The CCMs are an opportunity for the shortlisted Proponent and TTC to gain clarity on the following topic areas, with an objective of informing the shortlisted Proponent's optional BAFO resubmittal:

- Appendix G – Proposed Solution Submission Form;
- Appendix H – Pricing Submission Form; and,
- Appendix I – Form of Agreement Review Submission Form.

The Proponent was required to prepare and submit to TTC its proposed clarifications by topic area in accordance with the timetable to be provided to the shortlisted Proponent.

Shortlisted Proponent was responsible for taking their own notes during the CCMs. No minutes or notes will be issued by TTC to the shortlisted Proponents following the CCMs.

Following the CCMs, the shortlisted Proponent had the option of submitting any updates, if applicable, for Appendix H – Pricing Submission Form through the BAFO process, as described below. The shortlisted Proponent did submit a revised Appendix H – Pricing Submission Form through the BAFO process.

The process for Commercially Confidential Meetings conducted by the evaluation committee conformed to the process defined in the RFP.

6.8 STAGE VI Best and Final Offer

As per section 2.7 of the RFP, Stage VI allowed the shortlisted Proponent to revise their initial submissions received at the Submission Deadline and submit their BAFOs for final evaluation and ranking.

The shortlisted Proponent did submit a revised Appendix H – Pricing Submission Form through the BAFO process.

The Proponent's BAFO response was evaluated against the Rated Criteria set out in Part 4 – RFP Particulars, section E. Rated Criteria.

The process for Best and Final Offer conducted by the evaluation committee conformed to the process defined in the RFP.

6.9 STAGE VII Ranking and Contract Negotiations

As per section 2.8.1 of the RFP, after the completion of Stage VI, all of the revised scores from Stage VI will be added together and the shortlisted Proponents will be ranked based on their total scores. As only one proposal made it through all of the RFP stages it was deemed the top-ranked Proponent. IBM received a written invitation to enter into direct contract negotiations to finalize the agreement with TTC.

Evaluation Summary

The evaluation process conducted by the Evaluation Committee conformed to the process defined in the RFP and RFP Evaluation Framework. All Proponents' Proposals were treated fairly and evaluated in accordance with the evaluation criteria in the RFP and the RFP Evaluation Framework. We detected no bias or favouritism towards any Proponents. TTC's evaluation criteria and evaluation procedures were fairly and consistently applied and in accordance with the RFP and the RFP Evaluation Framework.

7 FINAL FAIRNESS REPORT

7.1 Review of Procurement Recommendation Report

As per our SOW P25PB21510, BDO was to provide a final fairness report on the Procurement Recommendation Report, which was created by TTC's Procurement & Category Management Department (PCM). On July 5, 2022 TTC provided BDO with the Procurement Recommendation Report, the RFP Commercial Analysis and the RFP MSS Scoring Summary documents for review.

As per the Procurement Recommendation Report, the PCM initiated negotiations with IBM on May 18, 2022 with support from Legal and ITS departments. As per our SOW, BDO did not take part in the contract negotiations between TTC and IBM.

CONTRACT AWARD PROCESS

Approval to award this contract is scheduled for the July 14, 2022 TTC Board meeting. Upon board approval and receipt of a procurement authorization by the CFO and CEO, PCM will issue an award letter and Purchase Order to IBM. The contract documents will be issued once the insurance documentation has been approved.