OCI
Request for Proposals for Cybersecurity Assessment and Plan

Ontario Centre of Innovation

325 Front Street West, Suite 300
Toronto, ON M5V 2Y1

416.861.1092 • 1.866.759.6014

oc-innovation.ca

Table of Contents

1. Organization Description

The **Ontario Centre of Innovation (OCI)**, established in 1987, is a leading not-for-profit organization that works with industry, academia and government.

OCI focuses on ensuring that the people of Ontario reap the personal and economic benefits of leading-edge research underway at our publicly funded universities, colleges and research hospitals - research that can be transformed into technologies and services that enhance quality of life and help build a globally competitive, job-creating economy in Ontario.

Specifically, OCI supports the commercialization of academic intellectual property (IP), industry-academic collaborations and the development and adoption of emerging technologies. This includes overseeing the execution of advanced technology platforms that will equip Ontario companies to compete in a competitive global digital economy.

We also support and invest in early-stage projects where the probability of commercial success and investment return on innovation are substantial. OCI's strong expertise in de-risking innovation helps attract private investors and other funders to new ventures, bolstering their success. We contribute as well to the development and retention of talent to ensure that industry has access to personnel with the most advanced skills and knowledge and that highly trained personnel find opportunities to apply their expertise in Ontario.

2. RFP Overview

2.1 Purpose of RFP

OCI has issued this Request for Proposal (RFP) to solicit responses from qualified technology security consulting firms (Proposers) offering proven Cyber Security Assessment services and the creation of Cyber Resilience Programs and Implementation Plans. OCI seeks a qualified Proposer who can demonstrate organizational, functional, and technical capabilities, as well as the experience, expertise, and qualifications necessary to fully audit and assess the security of OCI's current network and system environment, and then create a detailed Cyber Resilience Program (CRP) and Implementation Plan to strengthen our technology security and meet appropriate standards

2.2 Project Objective

With this RFP, OCI intends to fully assess and audit the security of all elements of the organization's technology environment. OCI's goal is to have a comprehensive and detailed review of the current environment, and then the creation of a Cyber Resilience Program (CRP) as well as an implementation plan to improve our overall technology security posture.

The Proposer should use IT industry standards to perform the assessment, including vulnerability assessments and penetration testing. A gap analysis should be used to demonstrate the effectiveness of current OCI IT infrastructure, security, and resourcing to identify and mitigate potential risk vulnerabilities.

The gap analysis will outline security weaknesses versus best practices and applicable policies and laws. Proposer is to provide the following:

- ✓ Threat level (high, medium, low)
- ✓ Level of effort to mitigate threat (high, medium, low)
- ✓ Estimated resource requirements to mitigate threats

Vendor's response shall demonstrate an understanding of the subject matter and describe the approach that will be taken to accomplish the services requested. In addition, the Proposer will need to provide a framework for a Cyber Resilience Program along with a Cyber Security Implementation Plan which together should include best practices guidance, needed technical configuration modifications, equipment, testing plans, and training. This plan should be tied to meeting, at a minimum, Government of Ontario Information Technology Standards (GO-ITS) and GO ITS 42 - Security Requirements for Enterprise Vulnerability Management

3. Scope of Services

OCI will select a qualified consultant on a best value basis, to undertake a comprehensive IT Cybersecurity Vulnerability Assessment, thoroughly reviewing the current state of the organization's information technology security, develop a vulnerability mitigation plan, and a prioritized road map of activities to enhance OCI's future Cybersecurity position. This outlines Phase 1 of the three sets of activities planned for enhancing cybersecurity at OCI summarized as below:

- Phase 1: Vulnerability Assessment
- Phase 2: Implementation
- Phase 3: Monitoring

The consultant's approach will utilize industry best practice methodologies to ensure a standardized risk mitigation approach that will offer the highest risk reduction potential.

The scope is to include, but not be limited to:

- ✓ Test for susceptibility to Advanced Persistent Threats (APTs) such as viruses, malware, Trojan horses, botnets and other targeted attack exploits. Evaluate OCI's current threat posture including antivirus and Intrusion Detection and Prevention (IDP) capabilities.

- ✓ Review OCI's current Supervisory Control and Data Acquisition (SCADA) for security vulnerabilities.
- ✓ Review wireless network system components for security vulnerabilities, validating system-specific configurations and known exploits.
- ✓ Validate system-specific configurations and review for known exploits. This includes firewalls, switches and routers, Microsoft Active Directory, email and file servers, web servers, wireless routers, VPN, VoIP and CCTV systems.
- ✓ Assess VoIP network system components for security vulnerabilities, validating system-specific configurations and reviewing for known exploits.
- ✓ Review existing IT policies and procedures and make recommendations for changes and/or additional policy and procedure development.
- ✓ Create and Implement Cybersecurity plan.
- ✓ Cybersecurity User Training: Suggest ongoing cybersecurity training for users by department / job function.

If these requirements are not met, the proposal will be removed from consideration.

The overall engagement will be managed by the vendor, with a defined scope, schedule and budget. Project activities will be appropriately managed, and project risks and task progress will be formally communicated. OCI will assign a Project Manager to act as a focal point for vendor communications.

Services will be provided at OCI's direction and discretion and may be provided in collaboration with OCI IT staff or third-party support vendors.

Services may be provided onsite or remotely, at the OCI's discretion.

3.1. Deliverables

Deliverables under Phase 1 will include:

I: Project Management Deliverables

a) Work Breakdown Schedule (WBS) including tasks
b) Schedule and dependencies
c) Weekly Status Reports including risks and progress reports.

II: Reporting

An executive summary detailing OCI's Cybersecurity position, including a comparative scorecard of findings; the results of vulnerability testing performed; identified cybersecurity vulnerabilities, gaps, and mitigation plans; a prioritized road map of activities, developed in conjunction with OCI staff, to enhance OCI's future cybersecurity position.

A slide-deck summarizing report and recommendations to be presented to OCI's senior management upon completion of the project.

III: Projected Solutions and Costs

a) Provide an estimated range, based upon previous experience, of the total services costs to implement the proposed solutions.
b) Include a Rate Sheet that specifies and itemizes the cost for each proposed component, including all licensing, support, maintenance, and hosting items
c) For subscription-based services, provide annual pricing

3.2 Vendor Requirements

✓ Vendor offices must reside within Canada and the assessment must be run from within Canada. Vendor cannot outsource to a 3rd party that is located outside of Canada. Indicate where your support center is located.
✓ Vendor to provide a firm fixed price estimate for Phase 1 of the activity outlined in this statement of work.
✓ Vendor must list how long after executing a contract they need to begin project.
✓ Vendor must supply resumes and/or other evidence of qualifications for senior level technical leadership and key personnel assigned to the project.
✓ Vendor must provide evidence of relevant certifications and training and demonstrate technical proficiency (via certifications) for cybersecurity expertise.
✓ Vendor to provide five references for cybersecurity projects that have been completed within the past 3 years (include completion date), that can be contacted.

4. Timeline

The following timeline must be considered when developing the project workplan as part of the proposer's response to this RFP. The proposer(s) must further identify the overall approach to the project, work details, and schedule to complete all the required project tasks detailed in Section 4 (Summary of Deliverables). It should be noted that the selected proposer will work with the internal project team to finalize the work plan and confirm the timeline.

- Pre-work and consultations by **October 15th, 2022**
- Assessment of Vulnerabilities by **November 18th, 2022**
- Draft Assessment Report for OCI review by **December 1st, 2022**
- Slide-deck summarizing report/recommendations presented to OCI's senior management team by **December 5th, 2022**
- Finalized Assessment Report by **December 15th, 2022**

5. Bidding Requirements

a. Financial: Firm fixed price estimate for Phase 1 of the activity outlined in this statement of work is to be provided.

b. Proposal: Descriptions of the approach and methodology. Detailed timelines and deliverables are to be provided. 30-minute interviews including a presentation on approach and methodology and Q&A may be scheduled with short-listed candidates.

c. Collaborative Bids: Consultants are welcome to submit collaborative bids in partnership with other vendors.

d. Service Level: Delivery of milestones on time and of a quality acceptable to OCI.

e. Expertise: CV and brief overview of proposed project role and responsibility for each team member along with their relevant experience and qualifications is to be provided.

f. Terms and Conditions.
- ✓ Any information provided by OCI either in this RFP or in subsequent verbal or written communications shall be considered confidential and for express use in the preparation of this proposal.
- ✓ All proposals submitted become the property of OCI and are to be received and held in confidence.
- ✓ All data collected and all resulting reports and publications prepared by the successful bidder will be the exclusive property of OCI.
- ✓ This RFP does not create an employment relationship. Individuals performing services required by the contract are not employees of OCI.
- ✓ Any changes to scope of services and associated costs following execution of contract must be submitted in writing and are subject to approval by OCI.
- ✓ Travel and travel reimbursement are not authorized for this acquisition.
- ✓ The successful bidder will be paid upon submission of proper invoices to OCI at the prices stipulated on the contract.
- ✓ Invoices will contain the contract number and reference number.

g. Conflict of Interest: Arms-Length relationship or disclosure of potential conflict of interest is required.

h. References: A minimum of 3 references with details of work completed are to be provided.

i. Evaluation Criteria: Proposals will be evaluated on the basis of:

Skills and Expertise (35%)

- ✓ Understanding of the project objectives and context.
- ✓ Qualifications and expertise.
- ✓ Relevant experience and references in developing strategies/roadmaps for public sector clients, as well as in research, future forecasting, and/or data analysis, preferably in automotive, technology and mobility sectors and/or the future of work.

Methodology (25%)

- ✓ Proposed approach and methodology to the project.
- ✓ How well does the proposal address RFP requirements.
- ✓ Management and organization of the assignment.
- ✓ Commitment to assignment timelines, deadline, and overall terms and conditions.

Cost (40%)

j. Submission Format: Proposals are to be submitted in free form electronically in Word and PDF format. Please have proposals named as "Company Name Submission CyberSecurity Assessment and Plan RFP_DD-MM-YYYY". The receipt will be confirmed via e-mail.

k. Contact: Send proposals submissions and any questions and additional information requests to **Dr. Sagar Prabhudev** at **sprabhudev@oc-innovation.ca**. Please note that any responses may be shared with all potential bidders.

l. Bidding Process and Schedule: The application deadline is **August 15th, 2022**. Short-listed candidates may be invited for an interview. Final selection is expected to be done by September 15th, 2022. We reserve the right not to award the contract to any of those submitting proposals, and we may seek further responses.

6. Environment

In order to help Proposers prepare their RFP responses, this section documents the existing technology environment. Vendors who have submitted an Intent to Bid will receive a high-level network diagram of OCI's infrastructure upon execution and return of the Non-Disclosure Agreement. The selected vendor will be required to execute a separate, similar, Non-Disclosure Agreement with OCI that covers this effort from start to finish, declaring that any information obtained as part of this study will not be released to anyone other than OCI. The following table identifies OCI's current technology standards:

Technology	Current Standard
Server Hardware	
Databases	
Desktop Hardware	
Email Server/Client	
Virtual Environment	
Browsers	
Storage Area Network	
Active Directory	
VPN	
Scanners	
Printers	
Internet • Bandwidth • Redundancy	

7. General Terms and Conditions

A. Collusion
- By submitting a response to the RFP, each Proposer represents and warrants that its response is genuine and not made in the interest of, or on behalf of, any person not named therein; that the Proposer has not directly induced or solicited any other person to submit a sham response or any other person to refrain from submitting a response; and that the Proposer has not in any manner sought collusion to secure any improper advantage over any other person submitting a response.

B. Gratuities

- No person will offer, give, or agree to give, any OCI employee or its representatives any gratuity, discount, or offer of employment in connection with the award of contract by OCI.

C. Required Review and Waiver of Protests

- Proposers should carefully review this RFP and all appendices, for comments, questions, defects, objections, or any other matter requiring clarification or correction (collectively called "comments"). Comments concerning RFP objections must be made in writing and received by OCI no later than the Timeline. This will allow issuance of any necessary amendments and help prevent the opening of defective Information upon which contract award could not be made. Protests based on any objection will be considered waived and invalid if these faults have not been brought to the attention of OCI in writing, by the Deadline for Proposer Questions.

D. Nondiscrimination

- No person will be excluded from participation in, be denied benefits of, be discriminated against in the admission or access to, or be discriminated against in treatment or employment in OCI's contracted programs or activities on the grounds of disability, age, race, color, religion, sex, national origin, or any other classification protected by Constitutional or statutory law; nor will they be excluded from participation in, be denied benefits of, or be otherwise subjected to discrimination in the performance of contracts with OCI or in the employment practices of the OCI's contractors. Accordingly, all Proposers entering into contracts with the OCI will, upon request, be required to show proof of such nondiscrimination and to post in conspicuous places, available to all employees and applicants, notices of nondiscrimination.

E. Proposal Preparation Costs

- The Proposer is responsible for any and all costs associated with the preparation, submittal, and presentation of any proposal.

F. Proposal Withdrawal

- To withdraw a proposal, the Proposer must submit a written request, signed by an authorized representative, to the RFP Coordinator identified in Section 5.K. After withdrawing a previously submitted proposal, the Proposer may submit another proposal at any time up to the deadline for submitting proposals.

G. Proposal Errors

- Proposers are liable for all errors or omissions contained in their proposals. Proposers will not be allowed to alter proposal documents after the deadline for submitting a proposal. OCI, at its discretion, has the right to accept or reject a proposal in part or whole due to errors and/or omissions of the response.

H. Incorrect Proposal Information

- If OCI determines that a Proposer has provided, for consideration in the evaluation process or contract negotiations, incorrect information which the Proposer knew or should have known was materially incorrect, that proposal may be determined non-responsive, and the proposal may be rejected at the sole discretion of OCI.

I. Prohibition of Proposer Terms and Conditions

- A Proposer may not submit the Proposer's own contract terms and conditions in a response to this RFP. If a proposal contains such terms and conditions, OCI, at its sole discretion, may determine the proposal to be a nonresponsive counter-offer, and the proposal may be rejected.

J. Assignment and Subcontracting

- Because of the sensitive nature of this type of project related OCI's technology environment, the Proposer may not subcontract, transfer, or assign any portion of the contract. The Proposer is prohibited from performing any work associated with this RFP or using offshore (outside Canada) resources for any service associated with this RFP.

K. Contract Negotiations

- After a review of the proposal, OCI intends to enter into contract negotiations with the selected Proposer. These negotiations could include all aspects of services and fees. If a contract is not finalized in a reasonable period of time, OCI reserves the right to open negotiations with an alternate Proposer.

L. Execution of Contract

- If the selected Proposer does not execute a contract with OCI within fifteen (15) business days after notification of selection, OCI may give notice to that service provider of OCI's intent to select from the remaining Proposers or to call for new Information, whichever OCI deems appropriate.

M. Right of Rejection

- OCI reserves the right, at its sole discretion, to reject any and all proposals or to cancel this RFP in its entirety. Any proposal received which does not meet the requirements of this RFP may be considered nonresponsive and the proposal may be rejected. Proposers must comply with all the terms of this RFP and all applicable laws and regulations. OCI may reject any proposal that does not comply with all the terms, conditions, and performance requirements of this RFP. Proposers may not restrict the rights of OCI or otherwise qualify their proposals. If a Proposer does so, OCI may determine the proposal to be a nonresponsive counter-offer, and the proposal may be rejected.