TABLE OF CONTENTS

PART 1 - GENERAL INFORMATION

1.1 Introduction

The bid solicitation is divided into seven parts plus attachments and annexes, as follows:

Part 1 General Information: provides a general description of the requirement;

Part 2 Bidder Instructions: provides the instructions, clauses and conditions applicable to the bid solicitation;

Part 3 Bid Preparation Instructions: provides Bidders with instructions on how to prepare their bid;

Part 4 Evaluation Procedures and Basis of Selection: indicates how the evaluation will be conducted, the evaluation criteria that must be addressed in the bid, and the basis of selection;

Part 5 Certifications and Additional Information: includes the certifications and additional information to be provided;

Part 6 Security, Financial and Other Requirements: includes specific requirements that must be addressed by Bidders; and

Part 7 Resulting Contract Clauses: includes the clauses and conditions that will apply to any resulting contract.

The Annexes include the Statement of Work, the Basis of Payment, and the Security Requirements Checklist.

1.2 Summary

The Canadian Defence Academy (CDA) is a branch within the Department of National Defence (DND), and the Canadian Armed Forces (CAF) responsible for the delivery of Professional Military Education. The Royal Military College (RMC) of Canada is a suborganization of CDA and is a provincially accredited university at the undergraduate and post-graduate level. RMC is made up of roughly 3,000 students, faculty staff, and administrative support staff. Similar to other provincial universities, RMC requires an academic network to enable the following functions, university teaching, undergraduate and graduate level research, and registrar function. The aim of this requisition is to allow CDA Communication Information Systems (CIS) to secure an intermediate-level External Network Penetration Testing (Pentest) Specialist who can work remotely, within the Solutions-Based Informatics Professional Services Supply Arrangement—Domains of Expertise: 10. Security Management BIPS SA - Domains of Expertise - Overview for SBIPS - Professional Services - Buying and Selling - PSPC (tpsgc-pwgsc.gc.ca)

1.2.2 There are security requirements associated with this requirement. For additional information, consult Part 6 - Security, Financial and Other Requirements, and Part 7 - Resulting Contract Clauses. For more information on personnel and organization security screening or security clauses, Bidders should refer to the Contract Security Program of Public Works and Government Services Canada (http://www.tpsgc-pwgsc.gc.ca/esc-src/introduction-eng.html) website.

1.3 Debriefings

Bidders may request a debriefing on the results of the bid solicitation process. Bidders should make the request to the Contracting Authority within 15 working days from receipt of the results of the bid solicitation process. The debriefing may be in writing, by telephone or in person.

PART 2 - BIDDER INSTRUCTIONS

2.1 Standard Instructions, Clauses and Conditions

All instructions, clauses and conditions identified in the bid solicitation by number, date and title are set out in the Standard Acquisition Clauses and Conditions Manual (https://buyandsell.gc.ca/policy-and-guidelines/standard-acquisition-clauses-and-conditions-manual) issued by Public Works and Government Services Canada.

Bidders who submit a bid agree to be bound by the instructions, clauses and conditions of the bid solicitation and accept the clauses and conditions of the resulting contract.

The 2003 (2023-06-08) Standard Instructions - Goods or Services - Competitive Requirements, are incorporated by reference into and form part of the bid solicitation.

2.2 Submission of Bids

Bids must be submitted only to Department of National Defence (DND) Bid Receiving Unit by the date, time and place indicated in the bid solicitation.

Due to the nature of the bid solicitation, bids transmitted by facsimile to DND will not be accepted.

2.3 Former Public Servant

Contracts awarded to former public servants (FPS) in receipt of a pension or of a lump sum payment must bear the closest public scrutiny, and reflect fairness in the spending of public funds. In order to comply with Treasury Board policies and directives on contracts awarded to FPSs, bidders must provide the information required below before contract award. If the answer to the questions and, as applicable the information required have not been received by the time the evaluation of bids is completed, Canada will inform the Bidder of a time frame within which to provide the information. Failure to comply with Canada's request and meet the requirement within the prescribed time frame will render the bid non-responsive.

Definitions

For the purposes of this clause, "former public servant" is any former member of a department as defined in the *Financial Administration Act*, R.S., 1985, c. F-11, a former member of the Canadian Armed Forces or a former member of the Royal Canadian Mounted Police. A former public servant may be:

(a) an individual;
(b) an individual who has incorporated;
(c) a partnership made of former public servants; or
(d) a sole proprietorship or entity where the affected individual has a controlling or major interest in the entity.

"lump sum payment period" means the period measured in weeks of salary, for which payment has been made to facilitate the transition to retirement or to other employment as a result of the implementation of various programs to reduce the size of the Public Service. The lump sum payment period does not include the period of severance pay, which is measured in a like manner.

"pension" means a pension or annual allowance paid under the *Public Service Superannuation Act* (PSSA), R.S., 1985, c. P-36, and any increases paid pursuant to the *Supplementary Retirement Benefits Act*, R.S., 1985, c. S-24 as it affects the PSSA. It does not include pensions payable pursuant to the *Canadian Forces Superannuation Act*, R.S., 1985, c. C-17, the *Defence Services Pension Continuation Act*, 1970, c. D-3, the *Royal Canadian Mounted Police Pension Continuation Act* , 1970, c. R-10, and the *Royal Canadian Mounted Police Superannuation Act*, R.S., 1985, c. R-11,

the *Members of Parliament Retiring Allowances Act*, R.S. 1985, c. M-5, and that portion of pension payable to the *Canada Pension Plan Act*, R.S., 1985, c. C-8.

"Cybersecurity" is defined as the body of technologies, processes, practices and response and mitigation measures designed to protect networks, computers, programs and data from attack, damage or unauthorized access so as to ensure confidentiality, integrity and availability.

Former Public Servant in Receipt of a Pension

As per the above definitions, is the Bidder a FPS in receipt of a pension? **Yes** ( ) **No** ( )

If so, the Bidder must provide the following information, for all FPSs in receipt of a pension, as applicable:
(a) name of former public servant;
(b) date of termination of employment or retirement from the Public Service.

By providing this information, Bidders agree that the successful Bidder's status, with respect to being a former public servant in receipt of a pension, will be reported on departmental websites as part of the published proactive disclosure reports in accordance with Contracting Policy Notice: 2019-01 and the Guidelines on the Proactive Disclosure of Contracts.

Work Force Adjustment Directive

Is the Bidder a FPS who received a lump sum payment pursuant to the terms of the Work Force Adjustment Directive? **Yes** ( ) **No** ( )

If so, the Bidder must provide the following information:
(a) name of former public servant;
(b) conditions of the lump sum payment incentive;
(c) date of termination of employment;
(d) amount of lump sum payment;
(e) rate of pay on which lump sum payment is based;
(f) period of lump sum payment including start date, end date and number of weeks;
(g) number and amount (professional fees) of other contracts subject to the restrictions of a work force adjustment program.

2.4 Enquiries - Bid Solicitation

All enquiries must be submitted in writing to the Contracting Authority no later than three (3) calendar days before the bid closing date. Enquiries received after that time may not be answered.

Bidders should reference as accurately as possible the numbered item of the bid solicitation to which the enquiry relates. Care should be taken by Bidders to explain each question in sufficient detail in order to enable Canada to provide an accurate answer. Technical enquiries that are of a proprietary nature must be clearly marked "proprietary" at each relevant item. Items identified as "proprietary" will be treated as such except where Canada determines that the enquiry is not of a proprietary nature. Canada may edit the question(s) or may request that the Bidder do so, so that the proprietary nature of the question(s) is eliminated and the enquiry can be answered to all Bidders. Enquiries not submitted in a form that can be distributed to all Bidders may not be answered by Canada.

2.5 Applicable Laws

Any resulting contract must be interpreted and governed, and the relations between the parties determined, by the laws in force in Onatraio.

Bidders may, at their discretion, substitute the applicable laws of a Canadian province or territory of their choice without affecting the validity of their bid, by deleting the name of the Canadian province or territory

specified and inserting the name of the Canadian province or territory of their choice. If no change is made, it acknowledges that the applicable laws specified are acceptable to the Bidders.

2.6 Bid Challenge and Recourse Mechanisms

(a) Several mechanisms are available to potential suppliers to challenge aspects of the procurement process up to and including contract award.

(b) Canada encourages suppliers to first bring their concerns to the attention of the Contracting Authority. Canada's Buy and Sell website, under the heading "Bid Challenge and Recourse Mechanisms" contains information on potential complaint bodies such as:

- Office of the Procurement Ombudsman (OPO)
- Canadian International Trade Tribunal (CITT)

(c) Suppliers should note that there are **strict deadlines** for filing complaints, and the time periods vary depending on the complaint body in question. Suppliers should therefore act quickly when they want to challenge any aspect of the procurement process.

PART 3 - BID PREPARATION INSTRUCTIONS

3.1 Bid Preparation Instructions

Due to the nature of the bid solicitation, bids transmitted by CPC Connect service and by facsimile will not be accepted.

Canada requests that bidders provide their bid in separately bound sections as follows:

Section I: Technical Bid (1 soft copies)

Section II: Financial Bid (1 soft copies)

Section III: Certifications (1 soft copies)

Section IV: Additional Information (1 soft copies)

If there is a discrepancy between the wording of the soft copy on electronic media and the hard copy, the wording of the hard copy will have priority over the wording of the soft copy."

Prices must appear in the financial bid only. No prices must be indicated in any other section of the bid.

Canada requests that bidders follow the format instructions described below in the preparation of

Section I: Technical Bid

In their technical bid, Bidders should demonstrate their understanding of the requirements contained in the bid solicitation and explain how they will meet these requirements. Bidders should demonstrate their capability and describe their approach in a thorough, concise and clear manner for carrying out the work.

The technical bid should address clearly and in sufficient depth the points that are subject to the evaluation criteria against which the bid will be evaluated. Simply repeating the statement contained in the bid solicitation is not sufficient. In order to facilitate the evaluation of the bid, Canada requests that Bidders address and present topics in the order of the evaluation criteria under the same headings. To avoid duplication, Bidders may refer to different sections of their bids by identifying the specific paragraph and page number where the subject topic has already been addressed.

Section II: Financial Bid

3.1.1 Bidders must submit their financial bid in accordance with the Basis of Payment in Annex B.

Section III: Certifications

3.1.2 Bidders must submit the certifications and additional information required under Part 5.

Section IV: Additional Information

PART 4 - EVALUATION PROCEDURES AND BASIS OF SELECTION

4.1 Evaluation Procedures

An evaluation team composed of representatives of Canada will evaluate the bids.

4.1.1 Technical Evaluation

4.1.1.1. Mandatory Technical Criteria

Item	Mandatory Criteria	Reference in Proposal	Met/Did Not Meet
M1	Must have a minimum of five (5) years' experience in the last ten (10) years in Cybersecurity – demonstrated by resume.		
M2	Must have demonstrated experience with performing penetration testing within the last three (3) years – demonstrated by references including Name, Position, Company, Phone and Email.		
M3	Must have performed one (1) penetration testing for organizations with at least 3,000 employees in the last three (3) years – demonstrated by references including Name, Position, Company, Phone and Email		
M4	Must have valid minimum Reliability Status Security Clearance for proposed resource – provide copy of certification.		
M5	Must have valid Certified Ethical Hacker (CEH) qualification – provide copy of certification.		

4.2 Basis of Selection

4.2.1 Mandatory Technical Criteria

SACC Manual Clause A0031T (2010-08-16), Basis of Selection – Mandatory Technical Criteria

A bid must comply with the requirements of the bid solicitation and meet all mandatory technical evaluation criteria to be declared responsive. The responsive bid with the lowest evaluated price will be recommended for award of a contract.

PART 5 – CERTIFICATIONS AND ADDITIONAL INFORMATION

Bidders must provide the required certifications and additional information to be awarded a contract.

The certifications provided by Bidders to Canada are subject to verification by Canada at all times. Unless specified otherwise, Canada will declare a bid non-responsive, or will declare a contractor in default if any certification made by the Bidder is found to be untrue, whether made knowingly or unknowingly, during the bid evaluation period or during the contract period.

The Contracting Authority will have the right to ask for additional information to verify the Bidder's certifications. Failure to comply and to cooperate with any request or requirement imposed by the Contracting Authority will render the bid non-responsive or constitute a default under the Contract.

5.1 Certifications Required with the Bid

Bidders must submit the following duly completed certifications as part of their bid.

5.1.1 Integrity Provisions - Declaration of Convicted Offences

In accordance with the Integrity Provisions of the Standard Instructions, all bidders must provide with their bid, **if applicable**, the Integrity declaration form available on the Forms for the Integrity Regime website (http://www.tpsgc-pwgsc.gc.ca/ci-if/declaration-eng.html), to be given further consideration in the procurement process.

5.2 Certifications Precedent to Contract Award and Additional Information

The certifications and additional information listed below should be submitted with the bid but may be submitted afterwards. If any of these required certifications or additional information is not completed and submitted as requested, the Contracting Authority will inform the Bidder of a time frame within which to provide the information. Failure to provide the certifications or the additional information listed below within the time frame specified will render the bid non-responsive.

5.2.1 Integrity Provisions – Required Documentation

In accordance with the section titled Information to be provided when bidding, contracting or entering into a real property agreement of the Ineligibility and Suspension Policy (http://www.tpsgc-pwgsc.gc.ca/ci-if/politique-policy-eng.html), the Bidder must provide the required documentation, as applicable, to be given further consideration in the procurement process.

5.2.2 Security Requirements – Required Documentation

In accordance with the requirements of the Contract Security Program of Public Works and Government Services Canada (http://www.tpsgc-pwgsc.gc.ca/esc-src/introduction-eng.html), the Bidder must provide a completed Contract Security Program Application for Registration (AFR) form to be given further consideration in the procurement process.

Bidders are reminded to obtain the required security clearance and, as applicable, security capabilities promptly. As indicated above, bidders who do not provide all the required information at bid closing will be given the opportunity to complete any missing information from the AFR form within a period set by the Contracting Authority. If that information is not provided within the timeframe established by the Contracting Authority (including any extension granted by the Contracting Authority in its discretion), or if Canada requires further information from the Bidder in connection with assessing the request for security clearance (i.e., information not required by the AFR form), the Bidder will be required to submit that information within the time period established by the Contracting Authority, which will not be less than 48 hours. If, at any time, the Bidder fails to provide the required information within the timeframe established by the Contracting Authority, its bid will be declared non-compliant.

PART 6 - SECURITY, FINANCIAL AND OTHER REQUIREMENTS

6.1 Security Requirements

6.1.1 Before award of a contract, the following conditions must be met:

(a) the Bidder must hold a valid organization security clearance as indicated in Part 7 - Resulting Contract Clauses;

6.1.2 Before access to sensitive information is provided to the Bidder, the following conditions must be met:

(a) the Bidder's proposed individuals requiring access to sensitive information, assets or sensitive work sites must meet the security requirements as indicated in Part 7 - Resulting Contract Clauses;
(b) the Bidder’s security capabilities must be met as indicated in Part 7 - Resulting Contract Clauses.

6.1.3 For additional information on security requirements, Bidders should refer to the Contract Security Program of Public Works and Government Services Canada (http://www.tpsgc-pwgsc.gc.ca/esc-src/introduction-eng.html) website.

PART 7 - RESULTING CONTRACT CLAUSES

The following clauses and conditions apply to and form part of any contract resulting from the bid solicitation.

7.1 Statement of Work

The Contractor must perform the Work in accordance with the Statement of Work at Annex A.

7.2 Standard Clauses and Conditions

All clauses and conditions identified in the Contract by number, date and title are set out in the Standard Acquisition Clauses and Conditions Manual (https://buyandsell.gc.ca/policy-and-guidelines/standard-acquisition-clauses-and-conditions-manual) issued by Public Works and Government Services Canada.

7.2.1 General Conditions

2035 (2022-12-01), General Conditions - Higher Complexity - Services, apply to and form part of the Contract.

7.2.2 Supplemental General Conditions

4010 (2022-12-01), Services: Higher complexity, apply to and form part of the Contract.

7.3 Security Requirements

7.3.1 The following security requirements (SRCL and related clauses provided by the Contract Security Program) apply and form part of the Contract:

7.3.2 The Contractor must, at all times during the performance of the Contract, hold a valid Designated Organization Screening (DOS), issued by the Contract Security Program (CSP), Public Works and Government Services Canada (PWGSC).

7.3.3 The Contractor personnel requiring access to sensitive site(s) must EACH hold a valid RELIABILITY STATUS, granted or approved by the CSP, PWGSC.

7.3.4 Subcontracts which contain security requirements are NOT to be awarded without the prior written permission of the CSP, PWGSC.

7.3.5 The Contractor must comply with the provisions of the:

7.3.5.1 Security Requirements Check List and security guide (if applicable), attached at Annex C;

7.3.5.2 Contract Security Manual (Latest Edition).

7.4 Term of Contract

7.4.1 Period of the Contract

The period of the Contract is from date of Contract Award to October 31st, 2023, inclusive.

7.4.2 Option to Extend the Contract

The Contractor grants to Canada the irrevocable option to extend the term of the Contract by up to one (1) additional one (1) year period(s) under the same conditions. The Contractor agrees that, during the

extended period of the Contract, it will be paid in accordance with the applicable provisions as set out in the Basis of Payment.

Canada may exercise this option at any time by sending a written notice to the Contractor at least fifteen (15) calendar days before the expiry date of the Contract. The option may only be exercised by the Contracting Authority, and will be evidenced for administrative purposes only, through a contract amendment.

7.5 Authorities

7.5.1 Contracting Authority

The Contracting Authority for the Contract is:

Name: _____
Title: _____
Acquisitions Branch
Directorate: _____
Address: _____
Telephone: ___-___-_____
E-mail address: _____

The Contracting Authority is responsible for the management of the Contract and any changes to the Contract must be authorized in writing by the Contracting Authority. The Contractor must not perform work in excess of or outside the scope of the Contract based on verbal or written requests or instructions from anybody other than the Contracting Authority.

7.5.2 Project Authority

The Project Authority for the Contract is:

Name: _____
Title: _____
Organization: _____
Address: _____
Telephone: ___-___-_____
E-mail address: _____

The Project Authority is the representative of the department or agency for whom the Work is being carried out under the Contract and is responsible for all matters concerning the technical content of the Work under the Contract. Technical matters may be discussed with the Project Authority; however, the Project Authority has no authority to authorize changes to the scope of the Work. Changes to the scope of the Work can only be made through a contract amendment issued by the Contracting Authority.

7.5.3 Contractor's Representative

Name: _____
Title: _____
Organization: _____
Address: _____
Telephone: ___-___-_____
E-mail address: _____

7.6 Proactive Disclosure of Contracts with Former Public Servants

By providing information on its status, with respect to being a former public servant in receipt of a *Public Service Superannuation Act* (PSSA) pension, the Contractor has agreed that this information will be reported on departmental websites as part of the published proactive disclosure reports, in accordance with Contracting Policy Notice: 2019-01 of the Treasury Board Secretariat of Canada.

7.7 Payment

7.7.1 Basis of Payment

Professional Fees

In consideration of the Contractor satisfactorily completing all of its obligations under the Contract, the Contractor will be paid a firm price of $ _____ (*insert amount at contract award*). Customs duties are included and Applicable Taxes are extra.

Other Direct Expenses

The Contractor will be reimbursed for the direct expenses reasonably and properly incurred in the performance of the Work. These expenses will be paid at actual cost without mark-up, upon submission of an itemized statement supported by receipt vouchers.

Estimated Cost: $_____

Total Estimated Contract Price : _____, Applicable Taxes extra.

Option to Extend the Contract

During the extended period of the Contract, the Contractor will be paid the firm price of $ _____ (*insert amount at contract award*) to perform all the Work in relation to the contract extension.

7.7.2 Limitation of Expenditure

Canada's total liability to the Contractor under the Contract must not exceed $ _____. Customs duties are included and Applicable Taxes are extra.

No increase in the total liability of Canada or in the price of the Work resulting from any design changes, modifications or interpretations of the Work, will be authorized or paid to the Contractor unless these design changes, modifications or interpretations have been approved, in writing, by the Contracting Authority before their incorporation into the Work. The Contractor must not perform any work or provide any service that would result in Canada's total liability being exceeded before obtaining the written approval of the Contracting Authority. The Contractor must notify the Contracting Authority in writing as to the adequacy of this sum:

(a) when it is 75% committed, or
(b) four months before the contract expiry date, or
(c) as soon as the Contractor considers that the contract funds provided are inadequate for the completion of the Work,

whichever comes first.

If the notification is for inadequate contract funds, the Contractor must provide to the Contracting Authority a written estimate for the additional funds required. Provision of such information by the Contractor does not increase Canada's liability.

7.7.3 Single Payment H1000C (2008-05-12)

Canada will pay the Contractor upon completion and delivery of the Work in accordance with the payment provisions of the Contract if:

(a) an accurate and complete invoice and any other documents required by the Contract have been submitted in accordance with the invoicing instructions provided in the Contract;
(b) all such documents have been verified by Canada;
(c) the Work delivered has been accepted by Canada.

7.7.4 Discretionary Audit

The estimated amount of profit included in the Contractor's price or rate certification is subject to audit by Canada, before or after payment is made to the Contractor under the conditions of the Contract. The purpose of the audit would be to determine whether the actual profit earned on a single contract if only one exists, or the aggregate of actual profit earned by the Contractor on a series of negotiated firm price and fixed-time rate contracts performed during a particular period selected, is reasonable and justifiable based on the estimated amount of profit included in earlier price or rate certification(s).

If the audit demonstrates that the actual profit is not reasonable and justifiable, as defined above, the Contractor must repay Canada the amount found to be in excess.

7.7.5 Time Verification

Time charged and the accuracy of the Contractor's time recording system are subject to verification by Canada, before or after payment is made to the Contractor. If verification is done after payment, the Contractor must repay any overpayment, at Canada's request.

7.8 Invoicing Instructions

The Contractor must submit invoices in accordance with the section entitled "Invoice Submission" of the general conditions. Invoices cannot be submitted until all work identified in the invoice is completed.
Instruction to contracting officers: Use the following paragraph when invoices must be accompanied by supporting documents. The documents listed are examples only and must be revised to reflect the requirement. Delete this paragraph if no supporting documents are required.
Each invoice must be supported by:

(a) a copy of time sheets to support the time claimed;

(b) a copy of the release document and any other documents as specified in the Contract;

(c) a copy of the invoices, receipts, vouchers for all direct expenses, and all travel and living expenses;

(d) a copy of the monthly progress report.

Invoices must be distributed as follows:

(a) The original and one (1) copy must be forwarded to the address shown on page 1 of the Contract for certification and payment.

7.9 Certifications and Additional Information

7.9.1 Compliance

Unless specified otherwise, the continuous compliance with the certifications provided by the Contractor in its bid or precedent to contract award, and the ongoing cooperation in providing additional information

are conditions of the Contract and failure to comply will constitute the Contractor in default. Certifications are subject to verification by Canada during the entire period of the Contract.

7.10 Applicable Laws

The Contract must be interpreted and governed, and the relations between the parties determined, by the laws in force in Ontario.

7.11 Priority of Documents

If there is a discrepancy between the wording of any documents that appear on the list, the wording of the document that first appears on the list has priority over the wording of any document that subsequently appears on the list.

(a) the Articles of Agreement;
(b) the supplemental general conditions 4010 (2022-12-01), Services: Higher complexity;
(c) the general conditions 2035 (2022-12-01), General Conditions - Higher Complexity - Services;
(d) Annex A, Statement of Work;
(e) Annex B, Basis of Payment;
(f) Annex C, Security Requirements Check List;
(g) the Contractor's bid dated _____,

7.12 Dispute Resolution

(a) The parties agree to maintain open and honest communication about the Work throughout and after the performance of the contract.
(b) The parties agree to consult and co-operate with each other in the furtherance of the contract and promptly notify the other party or parties and attempt to resolve problems or differences that may arise.
(c) If the parties cannot resolve a dispute through consultation and cooperation, the parties agree to consult a neutral third party offering alternative dispute resolution services to attempt to address the dispute.
(d) Options of alternative dispute resolution services can be found on Canada's Buy and Sell website under the heading "Dispute Resolution".

ANNEX A: STATEMENT OF WORK

1.0 BACKGROUND

1.1 The Canadian Defence Academy (CDA) is a branch within the Department of National Defence (DND), and the Canadian Armed Forces (CAF) responsible for the delivery of Professional Military Education. The Royal Military College (RMC) of Canada is a suborganization of CDA and is a provincially accredited university at the undergraduate and post-graduate level. RMC is made up of roughly 3,000 students, faculty staff, and administrative support staff. Similar to other provincial universities, RMC requires an academic network to enable the following functions, university teaching, undergraduate and graduate level research, and registrar function.

2.0 AIM

2.1 The aim of this Statement of Work is to allow CDA Communication Information Systems (CIS) to secure an intermediate-level External Network Penetration Testing (Pentest) Specialist who can work remotely, within the Solutions-Based Informatics Professional Services Supply Arrangement—Domains of Expertise: 10. Security Management BIPS SA - Domains of Expertise - Overview for SBIPS - Professional Services - Buying and Selling - PSPC (tpsgc-pwgsc.gc.ca)

3.0 REQUIREMENT

3.1 CDA CIS requires an intermediate-level External Network Penetration Testing Specialist with Certified Ethical Hacker (CEH) qualification to perform two (2) pentest. First pentest is an external network pentest to identify and exploit network and host-based security vulnerabilities within the internet-facing networked infrastructures operated by RMC. This pentest must follow the Penetration Testing Execution Standard (PTES) methodology. Second pentest is a web-application pentest of RMC internet-facing web-applications through unauthenticated and automated web-application scanning that must be compliant with Payment Card Industry (PCI) Data Security Standard (DSS). CDA CIS to identify which RMC web-application that will be targeted during the pentest, which shall be no fewer than seven (7) but shall not exceed a maximum of ten (10) web-application. This pentest must follow the Open Web Application Security Project (OWAS) methodology.

3.2 The Contractor resource during the external network pentest is to:

3.2.1 Device Discovery – Resource will establish a profile of Internet Protocol (IP) ranges provided by RMC to identify active external devices, which shall be no fewer than ten (10) active external devices but shall not exceed a maximum of thirty-five (35) active external devices.

3.2.2 Vulnerability Scanning – Resource will analyze available network services and IP stack fingerprints of all active external devices identified in the device discovery phase.

3.2.3 Vulnerability Validation – Resource will attempt to validate the results of vulnerability scanning to identify (and disregard) any false-positive results and validate other positive results from automated testing.

3.2.4 Exploitation – After establishing an understanding of external device roles, potential trust relationships, accessible network services, and potential vulnerabilities, resource will attempt to gain access to target systems.

3.2.5 Post-Exploitation – After completing exploitation phase and achieving access to any vulnerable hosts and data, the resource will attempt to escalate privileges on any exploited host(s). Resource will attempt to leverage this access and access to data (such

as password hashes and authentication tokens) on these hosts to gain additional access into the RMC network and attempt to access additional systems and data.

3.1 The Contractor resource during the web-application pentest is to:

3.3.1 Input Validation Bypass – Resource will remove client-side validation routines and bounds-checking restrictions to confirm controls are implemented on application parameters sent to the server.

3.3.2 SQL Injection – Resource will submit specially crafted SQL commands in input fields to validate input controls are in place for the protection of database data.

3.3.3 Cross-site Scripting – Resource will submit active content to the application in an attempt to cause a user's web browser to execute unauthorized and unfiltered code. This test is meant to validate user input controls.

3.3.4 Parameter Tampering - Resource will modify query strings and parameters and hidden fields in an attempt to gain unauthorized access to user data or application functionality.

3.3.5 Forceful Browsing – Resource will enumerate files located on a web server in an attempt to access files and user data not explicitly shown to the user within the application interface.

3.3.6 Backdoors and Debug Options – Resource will identify code left by developers for debugging purposes that could potentially allow an intruder to gain additional levels of access.

3.3.7 Configuration Subversion – Resource will assess RMC web servers and application servers for improper configurations that could create attack vectors.

4.0 LOCATION OF WORK

4.1 All work is expected to be completed remotely with any meetings taking place virtually.

5.0 LANGUAGE REQUIREMENT

5.1 Interaction will be in English.

6.0 TASKS AND DELIVERABLES

6.1 Tasks

6.1.1 The contractor resource must perform an external network pentest on RMC Network;

6.1.2 The contractor resource must provide outline of external network pentest plan following PTES methodology and have it approved by CDA CIS;

6.1.3 The contractor resource must complete the external network pentest in accordance with outline plan;

6.1.4 The contractor resource must perform a web-application pentest on RMC web-applications;

6.1.5 The contractor resource must provide outline of web-application pentest plan following OWASP methodology and have it approved by CDA CIS;

6.1.6 The contractor resource must complete the web-application pentest in accordance with approved outline plan;

6.1.7 The contractor resource must continuously document prioritized list of vulnerabilities, methodologies to exploit them, recommended corrective measures adapted to RMC's environment.

6.1.8 The contracted resource must provide, at a minimum, a weekly update report in writing to CDA CIS.

7.2 Deliverables

7.2.1 The contractor resource must document and provide an outline plan of external and web-application pentests in a format that is compatible with MS Office applications to CDA CIS, and provide consultation of outline plan to CDA CIS for approval prior to commencement of pentest; withing one(1) week of contract award..

7.2.2 The contractor resource must perform an external network pentest on RMC network, and a web-application pentest on RMC web-application within 2 weeks of contract award.

7.2.3 The contractor resource must provide pentest report documentation to include the following (but no limited to):

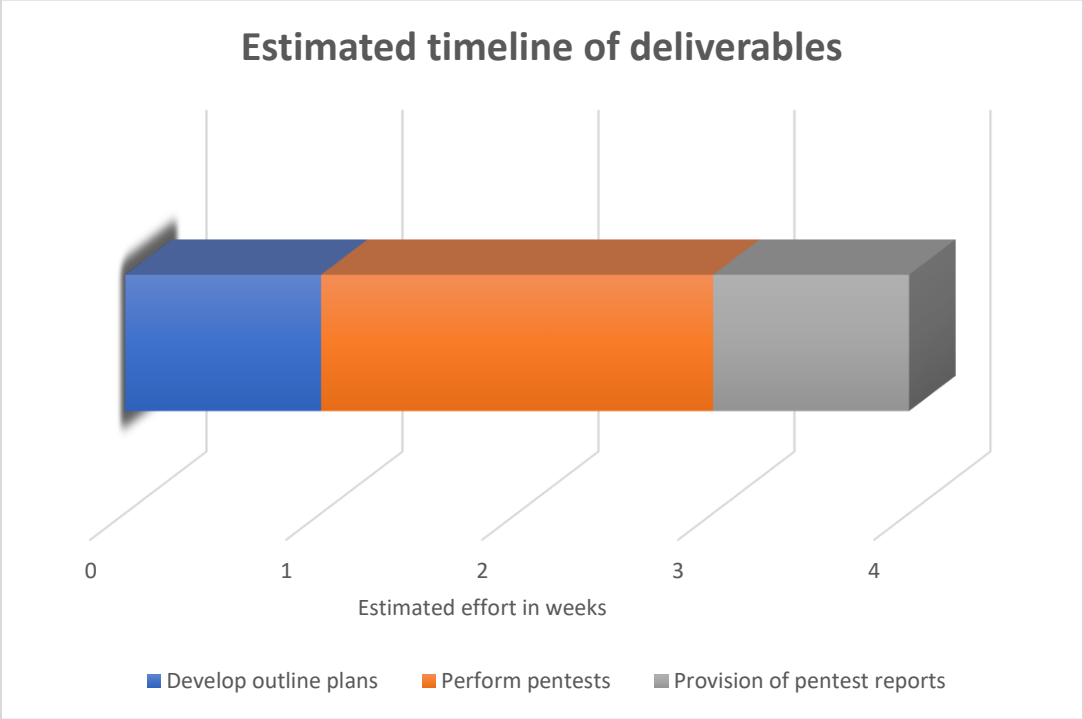
a. Executive summary;

b. Vulnerabilities technical details;

c. Testing methodologies;

d. Fixes and recommendations; and

e. Risk level..



9.0 DND RESPONSIBILITIES

9.1 DND will provide the following to the contractor:

9.1.1 Timely technical consultation and approvals within 24 hours from CDA CIS..

10.0 CONTRACTOR RESPONSIBILITIES

10.1 The Contractor is responsible to provide all IT and telecommunications assets required to carry out the work in this SOW.

Appendix #1 to Annex A: Royal Military College Academic Network (RMC Net)

1.0 Background

1.1 Modern university environments rely on a dynamic mix of computing infrastructure and network services to facilitate the core mission of the institution. For example, classroom/laboratory-based teaching in information-enabled spaces, learning spaces for individual and small group study and interaction, hosting academic workshops and symposiums, ad hoc meetings between academic researchers and administrative committees, etc. There are fixed laboratory computers and office workstations on the Royal Military College (RMC) campus that provide standard office productivity tools, access to RMC databases and administrative tools, and specialized laboratory and analytical software.

1.2 The contemporary university environment, and that of the foreseeable future, is dependent upon ubiquitous access to online information. In many ways online access to the world-wide web is as important to a contemporary university as its library. The availability of online information is fundamental to the dynamic ad hoc interaction of students, faculty, staff and researchers.

1.3 There are a wide variety of technology-based collaboration tools available that provide a range of collaboration experiences. Tools found within existing dedicated Learning Management Systems have been developed specifically to support the academic environment; such tools provide, by design, the necessary structure to support academic learning.

2.0 Royal Military College Academic Network (RMC Net)

2.1 The Royal Military College Academic Network (RMC Net) is an independent internet-facing network that acts as the primary education delivery and academic administration tool for the university functions of the Royal Military College (RMC). The network has a wide array of internet-facing services as RMC students, both undergraduate and post-graduate, primarily function in the Bring Your Own Device (BYOD) space. The network's applications contain both RMC's Learning Management System (Moodle based) and Student Information System (bespoke Oracle based applications) while supporting the full registrar functions of the university including admissions, scheduling and tuition payments for fee paying students. The network operates at the Protected A level while holding Protected B information, including Social Insurance Numbers, for generating tax slips. RMC Net is structured using Microsoft's Tier Model for Privileged Access Management (PAM), which creates separate tiers of admin accounts along with the implementation of Microsoft Local Administrator Password Solution (LAPS) to prevent the escalation of privileges and protect access to Tier 0 and Tier 1 services.

2.2 RMC Net is operated by both the Canadian Defence Academy's Computer Information Systems (CDA CIS) team and Shared Services Canada (SSC). The SSC Kingston Local Area Network (LAN) team is responsible for the operations of the RMC Net Wide Area Network (WAN) connection to the Internet through ORION and Bell connections, the RMC Net firewall and the RMC Net LAN. CDA CIS is responsible for server operations, application management, and desktop support.

3.0 RMC Administrative Environment

3.1 The Office of the Registrar is involved with a wide range of administrative functions, such as Attraction, Admission, Support to Undergraduate and Graduate programs, Governance and Prior Learning Assessment and Recognition (PLAR) assessment.

4.0 Attraction / Admissions

4.1 The Office of the Registrar is the first point of contact for potential students which starts by attracting potential students. From the perspective of computing resources, RMC maintain external web-sites. Included within the public audience for these web-sites will be other academics outside the colleges who will be seeking to develop research contacts.

4.2 The Office of the Registrar uses a number of commercial and bespoke applications to undertake the college administration:

4.2.1 Details of all registered students at both RMC and RMC-SJ are held in an application called CISA which is used by both Registrar staff and other personnel involved in the management and administration of students.

4.2.2 Establishing and maintaining class schedules also fall under the remit of the Office of the Registrar. Scheduling takes into account all teaching resources and schedules of students and staff. A key requirement of the scheduling capability is "agility"; schedules are required to be dynamic in order to respond to changing requirements from many different perspectives, e.g. students, staff, resource availability, IT, etc.

4.2.3 A "Degree Navigator" is available to both students and staff in order to facilitate the tracking of progress towards degree completion.

4.2.4 Student admission is coordinated between the College and the Canadian Forces Recruitment Group (CFRG); liaison between the two organisations is through the CFRIMS software located on the DWAN Enterprise network. Once a student has been registered all salient details are transferred to the internal CISA tool.

4.2.5 Where students are paying towards their education, there are provincial and federal requirements arising relating to OSAP and taxation that require students to retain access to their file following graduation in order to prepare submissions to the relevant authorities, e.g. students may require to submit Tax Form T2200 when preparing their tax returns following graduation.

4.2.6 The College has a statutory duty to accommodate students with disabilities to maximise students' chances of success. Such accommodation can require additional specialist software to be installed and used by students at relatively short notice.

4.3 The CISA application, by virtue of holding personal data, contains information regarded as "designated". Such information must be managed in a manner that compliant with relevant Government of Canada security policies relating to privacy and security, while supporting the reporting requirements of the Defence Analytics Programme.

5.0 Research

5.1 Research comprises an integral element of study at the higher-level graduate education. Academic research is the foundation for teaching at both undergraduate and graduate levels. The research environment is composed of Professors, Graduate Students, Post-Doctoral Fellows, Research Assistants, and Visiting Researchers; research is undertaken by groups sharing a common research goal, and results of that research written up in an academically rigorous fashion, for distribution within the institution.

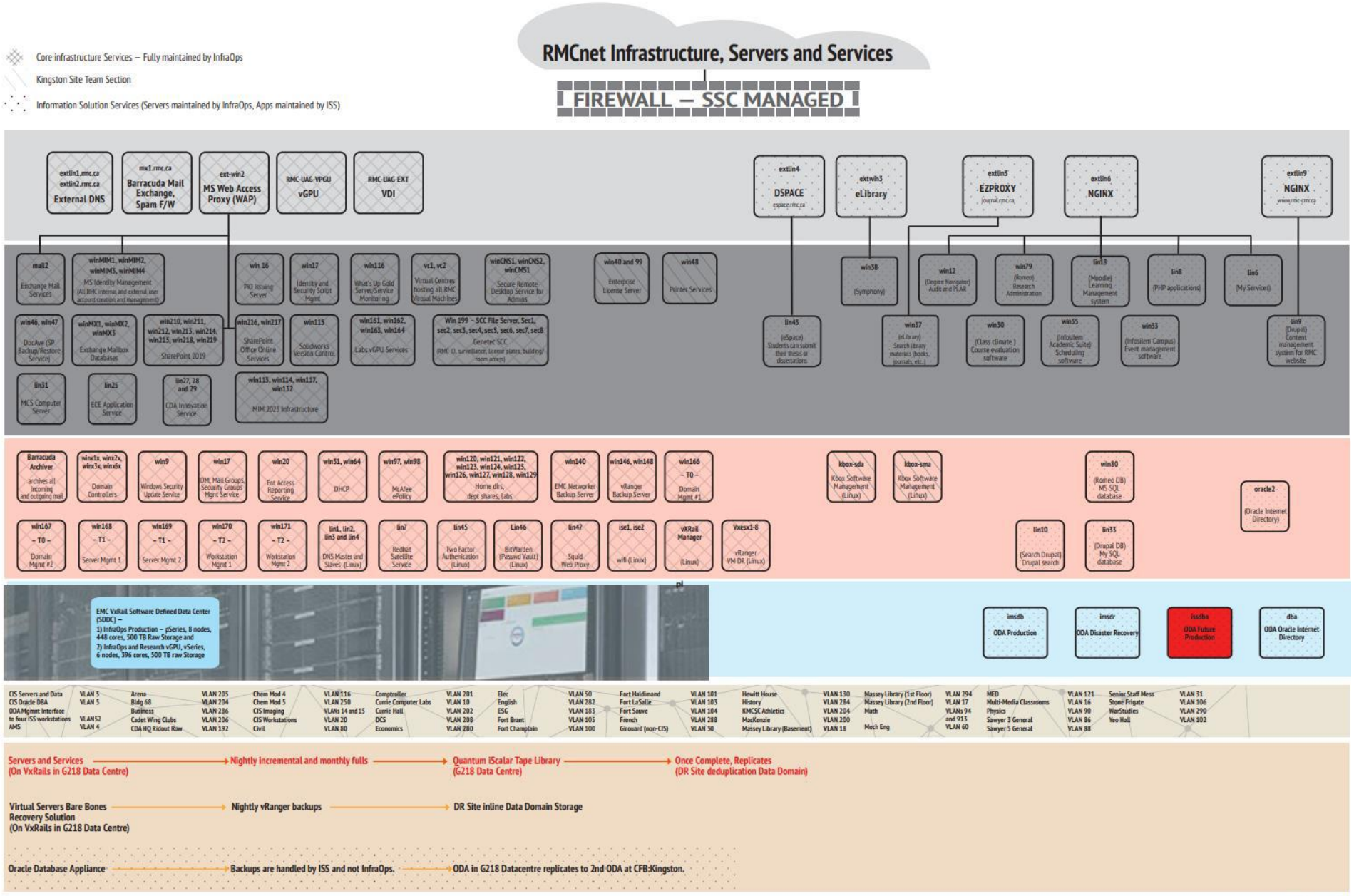
5.2 Research at RMC broadly aligns with the priorities of the CAF however faculty staff are guaranteed academic freedom under to undertake research as they see fit. This freedom includes not only the specific topics to be researched but also unfettered, unfiltered access to other networks and the tools and techniques used by researchers in the development of knowledge. From the perspective of computing resources, such freedom includes computing tools used for analysis and simulation as well as any specific instrumentation that may be required.; in the case of specialist instrumentation, this is often developed externally by specialist manufacturer; furthermore, the manufacturer may require remote access to the instrumentation to undertake maintenance and upgrades as the instrumentation evolves in parallel with the research.

5.3 The transition to digital formats for information storage has a number of consequent impacts;

- 5.3.1 streamed multi-media formats must be able to be viewed from a wide variety of trusted and public sources;
- 5.3.2 presentations have become rich, layered sources of information incorporating visuals and complex data sets;
- 5.3.3 analytical and statistical functions are also built into evolving software used in teaching and research.

6.0 Security and privacy

6.1 The requirements relating to information security and privacy appear to contradict the requirements for wireless access, BYOD, agility, flexibility, unfettered/unfiltered internet access and access to the network from external bodies outside the scope of Government of Canada clearances. In order to meet the necessary security and privacy requirements, RMC Net was structured using Microsoft’s Tier Model for PAM, and Microsoft LAPS was implemented.


Core infrastructure Services — Fully maintained by InfraOps
Kingston Site Team Section
Information Solution Services (Servers maintained by InfraOps, Apps maintained by ISS)
RMCnet Infrastructure, Servers and Services
FIREWALL — SSC MANAGED
DMZ
Application Servers
Core Infrastructure
Hardware
Network (SSC Managed) — See Annex A
Business Continuity
Disaster Recovery
External DNS
Barracuda Mail Exchange, Spam F/W
MS Web Access Proxy (WAP)
vGPU
VDI
DSPACE
eLibrary
EZPROXY
NGINX
Exchange Mail Services
MS Identity Management
PKI Issuing Server
Identity and Security Script Mgmt
What's Up Gold Server/Service Monitoring
Virtual Centres hosting all RMC Virtual Machines
Secure Remote Desktop Service for Admins
Enterprise License Server
Printer Services
(Symphony)
(Degree Navigator) Audit and PLAR
(Romeo) Research Administration
(Moodle) Learning Management system
(PHP applications)
(My Services)
DocAve (SP Backup/Restore Service)
Exchange Mail Boxes
Exchange Mailbox Databases
SharePoint 2019
SharePoint Office Online Services
Solidworks Version Control
Labs vGPU Services
Genetec SCC
(eSpace) Students can submit their thesis or dissertations
(eLibrary) Search library materials (books, journals, etc.)
(Class climate) Course evaluation software
(Infosilem Academic Suite) Scheduling software
(Infosilem Campus) Event management software
(Drupal) Content management system for RMC website
MCS Computer Server
ECE Application Service
CDA Innovation Service
MIM 2025 Infrastructure
Domain Controllers
Windows Security Update Service
DM, Mail Groups, Security Groups Mgmt Service
Ent Access Reporting Service
DHCP
McAfee ePolicy
Home dirs, dept shares, Labs
EMC Networker Backup Server
vRanger Backup Server
Domain Mgmt #1
Kbox Software Management (Linux)
(Romeo DB) MS SQL database
(Search Drupal) Drupal search
(Drupal DB) My SQL database
Domain Mgmt #2
Server Mgmt 1
Server Mgmt 2
Workstation Mgmt 1
Workstation Mgmt 2
DNS Master and Slaves (Linux)
Redhat Satellite Service
Two Factor Authenication (Linux)
BitWarden (Passwd Vault) (Linux)
Squid Web Proxy
wifi (Linux)
(Linux)
vRanger VM DR (Linux)
EMC VxRail Software Defined Data Center (SDDC) —
1) InfraOps Production — 9Series, 8 nodes, 448 cores, 500 TB Raw Storage and
2) InfraOps and Research vGPU, vSeries, 6 nodes, 396 cores, 500 TB raw Storage
ODA Production
ODA Disaster Recovery
ODA Future Production
ODA Oracle Internet Directory
Servers and Services (On VxRails in G218 Data Centre)
Nightly incremental and monthly fulls
Quantum iScalar Tape Library (G218 Data Centre)
Once Complete, Replicates (DR Site deduplication Data Domain)
Virtual Servers Bare Bones Recovery Solution (On VxRails in G218 Data Centre)
Nightly vRanger backups
DR Site inline Data Domain Storage
Oracle Database Appliance
Backups are handled by ISS and not InfraOps.
ODA in G218 Datacentre replicates to 2nd ODA at CFB:Kingston.
22 September 2021

Appendix #2 to Annex A: RMC Network Web-Application to be Penetration Tested

The following are internet and intranet sites that are within scope of the web-application penetration test:

services.rmc.ca (Mandatory)

Moodle.rmc.ca (Mandatory)

espace.rmc.ca

elibrary.rmc.ca

journal.rmc.ca

standards.rmc.ca

romeo.rmc.ca

dept.rmc.ca

collab.rmc.ca

www.rmc-cmr.ca (Mandatory)

ANNEX B: BASIS OF PAYMENT

The total not to exceed $_____ (applicable taxes not included) for services described in the Statement of Work (Annex A). Payment will follow the submission of an approved invoice.

Deliverable	Cost per hour	Level of Effort (hours)	Extended Cost
Two (2) External Network Penetration Testing (Pentests)	___/hr	**160 hours**	
		Subtotal:	
		Taxes (HST):	
		Total not to Exceed:	

Option Period:

Deliverable	Cost per hour	Level of Effort (hours)	Extended Cost
Additional External Network Penetration Testing Work	___/hr	**80 hours**	
		Subtotal:	
		Taxes (HST):	
		Total not to Exceed:	

ANNEX C: SECURITY REQUIREMENTS CHECK LIST
(SEE ATTACHED)