

TABLE DES MATIÈRES

PARTIE 1 – RENSEIGNEMENTS GÉNÉRAUX.....	2
1.1 INTRODUCTION.....	2
1.2 SOMMAIRE.....	2
1.3 COMPTE RENDU.....	3
PARTIE 2 – INSTRUCTIONS AUX SOUMISSIONNAIRES	4
2.1 INSTRUCTIONS, CLAUSES ET CONDITIONS UNIFORMISÉES	4
2.2 PRÉSENTATION DES SOUMISSIONS	4
2.3 ANCIEN FONCTIONNAIRE.....	4
2.4 DEMANDES DE RENSEIGNEMENTS – EN PÉRIODE DE SOUMISSION	5
2.5 LOIS APPLICABLES	6
2.6 PROCESSUS DE CONTESTATION DES SOUMISSIONS ET MÉCANISMES DE RECOURS	6
PARTIE 3 – INSTRUCTIONS POUR LA PRÉPARATION DES SOUMISSIONS	7
3.1 INSTRUCTIONS POUR LA PRÉPARATION DES SOUMISSIONS.....	7
PARTIE 4 – PROCÉDURES D'ÉVALUATION ET MÉTHODE DE SÉLECTION	8
4.1 PROCÉDURES D'ÉVALUATION.....	8
4.2 MÉTHODE DE SÉLECTION.....	9
PARTIE 5 – ATTESTATIONS ET RENSEIGNEMENTS SUPPLÉMENTAIRES.....	10
5.1 ATTESTATIONS EXIGÉES AVEC LA SOUMISSION.....	10
5.2 ATTESTATIONS PRÉALABLES À L'ATTRIBUTION DU CONTRAT ET RENSEIGNEMENTS SUPPLÉMENTAIRES	10
PARTIE 6 – EXIGENCES RELATIVES À LA SÉCURITÉ, EXIGENCES FINANCIÈRES ET AUTRES EXIGENCES	12
6.1 EXIGENCES RELATIVES À LA SÉCURITÉ	12
PARTIE 7 – CLAUSES DU CONTRAT SUBSÉQUENT.....	13
7.1 ÉNONCÉ DES TRAVAUX.....	13
7.2 CLAUSES ET CONDITIONS UNIFORMISÉES.....	13
7.3 EXIGENCES RELATIVES À LA SÉCURITÉ	13
7.4 DURÉE DU CONTRAT	13
7.5 RESPONSABLES.....	14
7.6 DIVULGATION PROACTIVE DES MARCHÉS CONCLUS AVEC D'ANCIENS FONCTIONNAIRES	15
7.7 PAIEMENT.....	15
7.8 INSTRUCTIONS RELATIVES À LA FACTURATION.....	16
7.9 ATTESTATIONS ET RENSEIGNEMENTS SUPPLÉMENTAIRES	17
7.10 LOIS APPLICABLES	17
7.11 ORDRE DE PRIORITÉ DES DOCUMENTS	17
7.12 RÈGLEMENT DES DIFFÉRENDS	17
ANNEXE A : ÉNONCÉ DES TRAVAUX.....	18
ANNEXE B : BASE DE PAIEMENT.....	29
ANNEXE C : LISTE DE VÉRIFICATION DES EXIGENCES RELATIVES À LA SÉCURITÉ (VOIR CI-JOINT).....	30

PARTIE 1 – RENSEIGNEMENTS GÉNÉRAUX

1.1 Introduction

La demande de soumissions contient sept parties, ainsi que des pièces jointes et des annexes, et elle est divisée comme suit :

Partie 1 Renseignements généraux : renferme une description générale du besoin;

Partie 2 Instructions à l'intention des soumissionnaires : renferme les instructions, les clauses et les conditions relatives à la demande de soumissions;

Partie 3 Instructions pour la préparation de la demande de soumission : donne aux soumissionnaires les instructions pour préparer leur soumission;

Partie 4 Procédures d'évaluation et méthode de sélection : décrit la façon selon laquelle se déroulera l'évaluation et présente les critères d'évaluation auxquels on doit répondre dans la soumission, ainsi que la méthode de sélection;

Partie 5 Attestations et renseignements supplémentaires : comprend les attestations et les renseignements supplémentaires à fournir;

Partie 6 Exigences relatives à la sécurité, exigences financières et autres exigences : comprend des exigences particulières auxquelles les soumissionnaires doivent répondre;

Partie 7 Clauses du contrat subséquent : contient les clauses et les conditions qui s'appliqueront à tout contrat subséquent.

Les annexes comprennent l'Énoncé des travaux, la Base de paiement et la Liste de vérification des exigences relatives à la sécurité.

1.2 Sommaire

L'Académie canadienne de la défense (ACD) est une direction générale du ministère de la Défense nationale (MDN) et des Forces armées canadiennes (FAC) chargée de la prestation de l'éducation militaire professionnelle. Le Collège militaire royal (CMR) du Canada est une sous-organisation de l'ACD et est une université provinciale accréditée au niveau du premier cycle et des études supérieures. Le CMR compte environ 3 000 étudiants, enseignants et personnel administratif. Comme d'autres universités provinciales, le CMR a besoin d'un réseau universitaire pour assurer les fonctions suivantes : l'enseignement universitaire, la recherche au niveau du premier cycle et des études supérieures, ainsi que la fonction du registraire. L'objectif de cette réquisition est de permettre aux systèmes d'information et de communication (SIC) de l'ACD d'assurer les services d'un spécialiste des tests d'intrusion des réseaux externes (Pentest) de niveau intermédiaire pouvant travailler à distance, dans le cadre de l'arrangement en matière d'approvisionnement en services professionnels en informatique centrés sur les solutions – domaines d'expertise : [10. Gestion de la sécurité PICS SA – Domaines d'expertise – Aperçu du SPICS – Services professionnels – Achat et vente – SPAC \(tpsgc-pwgsc.gc.ca\)](#)

1.2.2 Des exigences relatives à la sécurité sont associées à cette exigence. Pour plus de renseignements, consulter la partie 6 – Exigences relatives à la sécurité, exigences financières et autres exigences, et la partie 7 – Clauses du contrat subséquent. Pour plus de renseignements sur le processus d'enquête de sécurité du personnel et de l'organisation ou sur les clauses de sécurité, les soumissionnaires peuvent se référer au [Programme de sécurité des contrats](#) du site Web de Travaux publics et Services gouvernementaux Canada (<https://www.tpsgc-pwgsc.gc.ca/esc-src/introduction-fra.html>).

1.3 Compte rendu

Les soumissionnaires peuvent demander un compte rendu des résultats du processus d'appel d'offres. Les soumissionnaires doivent en faire la demande à l'autorité contractante dans les quinze (15) jours ouvrables suivant la réception des résultats du processus de demande de soumission. Le compte rendu peut se faire par écrit, par téléphone ou en personne.

PARTIE 2 – INSTRUCTIONS AUX SOUMISSIONNAIRES

2.1 Instructions, clauses et conditions uniformisées

Toutes les instructions, clauses et conditions indiquées dans la demande de soumission par un numéro, une date et un titre sont reproduites dans le [Guide des clauses et conditions uniformisées d'achat](https://achatsetventes.gc.ca/politiques-et-lignes-directrices/guide-des-clauses-et-conditions-uniformisees-d-achat) (<https://achatsetventes.gc.ca/politiques-et-lignes-directrices/guide-des-clauses-et-conditions-uniformisees-d-achat>) publié par Travaux publics et Services gouvernementaux Canada.

Les soumissionnaires qui présentent une soumission acceptent de respecter les instructions, les clauses et les conditions de la demande de soumission et acceptent les clauses et les conditions du contrat subséquent.

Le document Instructions uniformisées – biens ou services – besoins concurrentiels [2003](#) (2023-06-08) est incorporé par renvoi à la demande de soumission et en fait partie intégrante.

2.2 Présentation des soumissions

Les offres doivent être présentées uniquement à l'unité réceptrice des soumissions du ministère de la Défense nationale (MDN) au plus tard à la date, à l'heure et à l'endroit indiqués dans la demande de soumissions.

En raison de la nature de la demande de soumission, les soumissions transmises par télécopie au MDN ne seront pas acceptées.

2.3 Ancien fonctionnaire

Les contrats attribués à d'anciens fonctionnaires qui touchent une pension ou qui ont reçu un paiement forfaitaire doivent résister à l'examen scrupuleux du public et constituer une dépense équitable des fonds publics. Afin de respecter les politiques et les directives du Conseil du Trésor sur les contrats attribués à d'anciens fonctionnaires, les soumissionnaires doivent fournir l'information exigée ci-dessous avant l'attribution du contrat. Si la réponse aux questions et, s'il y a lieu, les renseignements requis n'ont pas été reçus au moment où l'évaluation des soumissions est terminée, le Canada informera le soumissionnaire d'un délai dans lequel il devra fournir les renseignements. Le défaut de se conformer à la demande du Canada et de satisfaire à l'exigence dans le délai prescrit rendra la soumission non recevable.

Définitions

Aux fins de cette clause, « ancien fonctionnaire » signifie tout ancien employé d'un ministère au sens de la [Loi sur la gestion des finances publiques](#), L.R., 1985, ch. F-11, un ancien membre des Forces armées canadiennes ou de la Gendarmerie royale du Canada. Un ancien fonctionnaire peut être :

- (a) un individu;
- (b) un individu qui s'est incorporé;
- (c) une société constituée d'anciens fonctionnaires; ou
- (d) une entreprise à propriétaire unique ou une entité dans laquelle la personne visée détient un intérêt important ou majoritaire.

« période de paiement forfaitaire » désigne la période mesurée en semaines de salaire à l'égard de laquelle un paiement a été fait pour faciliter la transition vers la retraite ou vers un autre emploi à la suite de la mise en place de divers programmes visant à réduire la taille de la fonction publique. La période du paiement forfaitaire ne comprend pas la période visée par l'allocation de fin de services, qui se mesure de façon similaire.

« pension » signifie une pension ou une allocation annuelle versée en vertu de la [Loi sur la pension de la fonction publique](#) (LPFP), L.R.C., 1985, ch. P-36, et toute augmentation versée en vertu de la [Loi sur les](#)

prestations de retraite supplémentaires, L.R., 1985, ch. S-24, dans la mesure où elle touche la LPFP. Elle ne comprend pas les pensions payables en vertu de la Loi sur la pension de retraite des Forces canadiennes, L.R., 1985, ch. C-17, de la Loi sur la continuation de la pension des services de défense 1970, ch. D-3, de la Loi sur la continuation des pensions de la Gendarmerie royale du Canada, 1970, ch. R-10, et de la Loi sur la pension de retraite de la Gendarmerie royale du Canada L.R.C., 1985, ch. R-11, de la Loi sur les allocations de retraite des parlementaires, L.R.C., 1985, ch. M-5, et la partie de la pension payable à la Loi sur le Régime de pensions du Canada L.R.C., 1985, ch. C-8.

« cybersécurité » est définie comme ensemble des technologies, des processus, des pratiques et des mesures d'atténuation et d'intervention conçus pour protéger les réseaux, les ordinateurs, les programmes et les données contre les attaques, les dommages ou les accès non autorisés afin d'assurer la confidentialité, l'intégrité et la disponibilité.

Ancien fonctionnaire touchant une pension

Selon les définitions ci-dessus, est-ce que le soumissionnaire est un ancien fonctionnaire qui touche une pension? **Oui () Non ()**

Dans l'affirmative, le soumissionnaire doit fournir les renseignements suivants, pour tous les anciens fonctionnaires touchant une pension, le cas échéant :

- (a) le nom de l'ancien fonctionnaire;
- (b) la date de cessation d'emploi dans la fonction publique ou de la retraite.

En fournissant ces renseignements, les soumissionnaires acceptent que le statut du soumissionnaire retenu, en tant qu'ancien fonctionnaire touchant une pension, figure dans les rapports de divulgation proactive des contrats, sur les sites Web des ministères, et ce, conformément à l'Avis sur la Politique des marchés : 2019-01 et aux Lignes directrices sur la divulgation proactive des marchés.

Directive sur le réaménagement des effectifs

Est-ce que le soumissionnaire est un ancien fonctionnaire qui a reçu un paiement forfaitaire en vertu de la Directive sur le réaménagement des effectifs? **Oui () Non ()**

Si oui, le soumissionnaire doit fournir les renseignements suivants :

- (a) le nom de l'ancien fonctionnaire;
- (b) les conditions de l'incitatif de paiement forfaitaire;
- (c) la date de la cessation d'emploi;
- (d) le montant du paiement forfaitaire;
- (e) le taux de rémunération qui a servi au calcul du paiement forfaitaire;
- (f) la période correspondant au paiement forfaitaire, incluant la date du début, d'achèvement et le nombre de semaines;
- (g) le nombre et le montant (honoraires professionnels) des autres contrats assujettis aux conditions d'un programme de réaménagement des effectifs.

2.4 Demandes de renseignements – en période de soumission

Toutes les demandes de renseignements doivent être présentées par écrit à l'autorité contractante au moins trois (3) jours civils avant la date de clôture des soumissions. Pour ce qui est des demandes de renseignements reçues après ce délai, il est possible qu'on ne puisse pas y répondre.

Les soumissionnaires doivent citer le plus fidèlement possible le numéro de l'article de la demande de soumissions sur lequel porte la demande de renseignements et prendre soin d'énoncer chaque question de manière suffisamment détaillée pour que le Canada puisse y répondre avec exactitude. Les demandes de renseignements techniques qui ont un caractère exclusif doivent porter clairement la mention « exclusif » vis-à-vis de chaque article pertinent. Les éléments portant la mention « exclusif » feront l'objet d'une discrétion absolue, sauf dans les cas où le Canada considère que la demande de

renseignements n'a pas un caractère exclusif. Dans ce cas, le Canada peut réviser les questions ou peut demander au soumissionnaire de le faire, afin d'en éliminer le caractère exclusif, et de permettre la transmission des réponses à tous les soumissionnaires. Le Canada peut ne pas répondre aux demandes de renseignements dont la formulation ne permet pas de les diffuser à tous les soumissionnaires.

2.5 Lois applicables

Tout contrat subséquent doit être interprété et régi selon les lois en vigueur en Ontario, et les relations entre les parties seront déterminées par ces lois.

À leur discrétion, les soumissionnaires peuvent indiquer les lois applicables d'une province ou d'un territoire canadien de leur choix, sans que la validité de leur soumission soit mise en question, en supprimant le nom de la province ou du territoire canadien précisé et en insérant le nom de la province ou du territoire canadien de leur choix. Si aucun changement n'est indiqué, cela signifie que les soumissionnaires acceptent les lois applicables indiquées.

2.6 Processus de contestation des soumissions et mécanismes de recours

- (a) Les fournisseurs potentiels ont accès à plusieurs mécanismes pour contester des aspects du processus d'approvisionnement jusqu'à l'attribution du contrat, inclusivement.
- (b) Le Canada invite les fournisseurs à porter d'abord leurs préoccupations à l'attention de l'autorité contractante. Le site Web « [Achats et ventes](#) » du Canada, sous la rubrique « [Processus de contestation des soumissions et mécanismes de recours](#) », fournit de l'information sur les organismes de traitement des plaintes possibles, notamment :
 - Bureau de l'ombudsman de l'approvisionnement (BOA)
 - Tribunal canadien du commerce extérieur (TCCE)
- (c) Les fournisseurs devraient savoir que des **délais stricts** sont fixés pour le dépôt des plaintes et qu'ils varient en fonction de l'organisation concernée. Les fournisseurs doivent donc agir rapidement lorsqu'ils souhaitent contester un aspect du processus d'approvisionnement.

PARTIE 3 – INSTRUCTIONS POUR LA PRÉPARATION DES SOUMISSIONS

3.1 Instructions pour la préparation des soumissions

En raison du caractère de la demande de soumissions, les soumissions transmises par le service Connexion de la SCP ou par télécopieur ne seront pas acceptées.

Le Canada demande aux soumissionnaires de fournir leur soumission en sections distinctes comme suit :

Section I : Soumission technique (1 copie électronique)

Section II : Soumission financière (1 copie électronique)

Section III : Attestations (1 copie électronique)

Section IV : Renseignements supplémentaires (1 copie électronique)

En cas d'incompatibilité entre le libellé de la copie électronique sur le média et de la copie papier, le libellé de la copie papier l'emportera sur celui de la copie électronique.

Les prix doivent figurer dans la soumission financière seulement. Aucun prix ne doit être indiqué dans une autre section de la soumission.

Le Canada demande que les soumissionnaires suivent les instructions de présentation décrites ci-dessous pour la préparation de

Section I : Soumission technique

Dans leur soumission technique, les soumissionnaires doivent démontrer qu'ils comprennent les exigences contenues dans la demande de soumissions et expliquer comment ils répondront à ces exigences. Les soumissionnaires doivent démontrer leur capacité et décrire l'approche qu'ils prendront de façon complète, concise et claire pour effectuer les travaux.

La soumission technique doit présenter clairement et de manière suffisamment détaillée les points sur lesquels portent les critères d'évaluation qui serviront à évaluer la soumission. Il ne suffit pas de simplement reprendre les énoncés contenus dans l'appel d'offres. Pour faciliter l'évaluation des soumissions, le Canada enjoint aux soumissionnaires de reprendre les sujets dans l'ordre des critères d'évaluation, sous les mêmes rubriques. Pour éviter les répétitions, les soumissionnaires peuvent faire des renvois aux différents articles de leur offre en indiquant le numéro du paragraphe et de la page où le sujet visé est déjà traité.

Section II : Soumission financière

3.1.1 Les soumissionnaires doivent présenter leur soumission financière conformément à en conformité avec la base de paiement figurant à l'annexe B.

Section III : Attestations

3.1.2 Les soumissionnaires doivent présenter les attestations et les renseignements supplémentaires exigés à la partie 5.

Section IV : Renseignements supplémentaires

PARTIE 4 – PROCÉDURES D'ÉVALUATION ET MÉTHODE DE SÉLECTION

4.1 Procédures d'évaluation

Une équipe d'évaluation composée de représentants du Canada évaluera les soumissions.

4.1.1 Évaluation technique

4.1.1.1 Critères techniques obligatoires

Élément	Critères obligatoires	Référence dans la proposition	Satisfait/Ne satisfait pas
O1	Doit avoir au moins cinq (5) ans d'expérience au cours des dix (10) dernières années dans le domaine de la cybersécurité – attestée par le curriculum vitae.		
O2	Avoir une expérience avérée des tests d'intrusion au cours des trois (3) dernières années, attestée par des références comprenant le nom, le poste, l'entreprise, le téléphone et l'adresse électronique.		
O3	Doit avoir effectué un (1) test d'intrusion pour un organisme comptant au moins 3 000 employés au cours des trois (3) dernières années – démontré par des références comprenant le nom, le poste, l'entreprise, le téléphone et l'adresse électronique.		
O4	Doit avoir une habilitation de sécurité minimale de fiabilité valide pour la ressource proposée – fournir une copie de la certification.		
O5	Doit avoir une certification valide de Certified Ethical Hacker (CEH) – fournir une copie de la certification.		

4.2 Méthode de sélection

4.2.1 Critères techniques obligatoires

Clause du *Guide CCUA* [A0031T](#) (16-08-2010), Base de sélection – Critères techniques obligatoires.

Une soumission doit respecter les exigences de la demande de soumissions et satisfaire à tous les critères d'évaluation technique obligatoires pour être déclarée recevable. La soumission recevable avec le prix évalué le plus bas sera recommandée pour attribution d'un contrat.

Solicitation No. - N° de l'invitation

W4938-23-073S

Client Ref. No. - N° de réf. du client

Amd. No. - N° de la modif.

File No. - N° du dossier

Buyer ID - Id de l'acheteur

Wood.JMS

CCC No./N° CCC - FMS No./N° VME

PARTIE 5 – ATTESTATIONS ET RENSEIGNEMENTS SUPPLÉMENTAIRES

Les soumissionnaires doivent fournir les attestations et les renseignements supplémentaires exigés pour qu'un contrat leur soit attribué.

Les attestations que les soumissionnaires remettent au Canada peuvent faire l'objet d'une vérification à tout moment par le Canada. À moins d'indication contraire, le Canada déclarera une soumission non recevable, ou à un manquement de la part de l'entrepreneur s'il est établi qu'une attestation du soumissionnaire est fautive, sciemment ou non, que ce soit pendant la période d'évaluation des soumissions, ou pendant la durée du contrat.

L'autorité contractante aura le droit de demander des renseignements supplémentaires pour vérifier les attestations du soumissionnaire. À défaut de répondre et de coopérer à toute demande ou exigence imposée par l'autorité contractante, la soumission sera déclarée non recevable, ou constituera un manquement aux termes du Contrat.

5.1 Attestations exigées avec la soumission

Les soumissionnaires doivent fournir les attestations suivantes dûment remplies avec leur soumission.

5.1.1 Dispositions relatives à l'intégrité – déclaration de condamnation à une infraction

Conformément aux dispositions relatives à l'intégrité des instructions uniformisées, tous les soumissionnaires doivent présenter avec leur soumission, **s'il y a lieu**, le formulaire de déclaration d'intégrité accessible sur le site Web [Intégrité – Formulaire de déclaration](http://www.tpsgc-pwgsc.gc.ca/ci-if/declaration-fra.html) (<http://www.tpsgc-pwgsc.gc.ca/ci-if/declaration-fra.html>), afin que leur soumission ne soit pas rejetée du processus d'approvisionnement.

5.2 Attestations préalables à l'attribution du contrat et renseignements supplémentaires

Les attestations et les renseignements supplémentaires énumérés ci-dessous doivent être fournis avec la soumission, mais ils peuvent être fournis plus tard. Si l'une de ces attestations ou l'un de ces renseignements supplémentaires ne sont pas remplis et fournis comme demandé, l'autorité contractante informera le soumissionnaire du délai à l'intérieur duquel les renseignements doivent être fournis. À défaut de fournir les attestations ou les renseignements supplémentaires énumérés ci-dessous dans le délai prévu, la soumission sera déclarée non recevable.

5.2.1 Dispositions relatives à l'intégrité – documentation exigée

Conformément à l'article intitulé Renseignements à fournir lors d'une soumission, de la passation d'un contrat ou de la conclusion d'un accord immobilier de la [Politique d'inadmissibilité et de suspension](http://www.tpsgc-pwgsc.gc.ca/ci-if/politique-policy-fra.html) (<http://www.tpsgc-pwgsc.gc.ca/ci-if/politique-policy-fra.html>), le soumissionnaire doit présenter la documentation exigée, s'il y a lieu, afin que sa soumission ne soit pas rejetée dans le cadre du processus d'approvisionnement.

5.2.2 Exigences relatives à la sécurité – Documentation requise

Conformément aux [exigences du Programme de sécurité des contrats](https://www.tpsgc-pwgsc.gc.ca/esc-src/introduction-fra.html) de Travaux publics et Services gouvernementaux Canada (<https://www.tpsgc-pwgsc.gc.ca/esc-src/introduction-fra.html>), le soumissionnaire doit fournir un formulaire de demande d'inscription au Programme de sécurité des contrats (PSC) dûment rempli pour que sa candidature soit prise en considération dans le cadre de processus d'approvisionnement.

Il est rappelé aux soumissionnaires qu'ils doivent obtenir rapidement l'attestation de sécurité requise et, le cas échéant, les capacités de sécurité. Comme il est indiqué ci-dessus, les soumissionnaires qui ne fournissent pas tous les renseignements requis à la clôture des soumissions auront la possibilité de

compléter les renseignements manquants du FDI dans un délai fixé par l'autorité contractante Si ces renseignements ne sont pas fournis dans le délai établi par l'autorité contractante (y compris toute prolongation accordée par l'autorité contractante à sa discrétion), ou si le Canada a besoin d'autres renseignements de la part du soumissionnaire dans le cadre de l'évaluation de la demande d'autorisation de sécurité (c.-à-d. des renseignements qui ne sont pas exigés par le FDI), le soumissionnaire sera tenu de soumettre ces renseignements dans le délai établi par l'autorité contractante, qui ne sera pas inférieur à 48 heures. Si, à quelque moment que ce soit, le soumissionnaire ne fournit pas les renseignements requis dans les délais fixés par l'autorité contractante, sa soumission sera déclarée non conforme.

PARTIE 6 – EXIGENCES RELATIVES À LA SÉCURITÉ, EXIGENCES FINANCIÈRES ET AUTRES EXIGENCES

6.1 Exigences relatives à la sécurité

6.1.1 Avant l'attribution d'un contrat, les conditions suivantes doivent être respectées :

- (a) le soumissionnaire doit détenir une attestation de sécurité d'organisation valable, comme indiqué à la Partie 7 – Clauses du contrat subséquent;

6.1.2 Avant que l'accès aux renseignements sensibles ne soit accordé au soumissionnaire, les conditions suivantes doivent être remplies :

- (a) les personnes proposées par le soumissionnaire qui doivent avoir accès à des renseignements ou à des biens de nature protégée ou classifiée ou à des établissements de travail dont l'accès est réglementé doivent posséder une attestation de sécurité, comme indiqué à la Partie 7 – Clauses du contrat subséquent;
- (b) les capacités de sécurité du soumissionnaire doivent être satisfaites, comme indiqué dans la partie 7 – Clauses du contrat subséquent.

6.1.3 Pour de plus amples renseignements sur les exigences relatives à la sécurité, les soumissionnaires doivent consulter le site Web du [Programme de sécurité des contrats](https://www.tpsgc-pwgsc.gc.ca/esc-src/introduction-fra.html) de Travaux publics et Services gouvernementaux Canada (<https://www.tpsgc-pwgsc.gc.ca/esc-src/introduction-fra.html>).

PARTIE 7 – CLAUSES DU CONTRAT SUBSÉQUENT

Les clauses et conditions suivantes s'appliquent à tout contrat subséquent découlant de la demande de soumissions et en font partie intégrante.

7.1 Énoncé des travaux

L'entrepreneur doit exécuter les travaux conformément à l'énoncé des travaux figurant à l'annexe A.

7.2 Clauses et conditions uniformisées

Toutes les clauses et conditions mentionnées dans le contrat par un numéro, une date et un titre sont reproduites dans le [Guide des clauses et conditions uniformisées d'achat](https://achatsetventes.gc.ca/politiques-et-lignes-directrices/guide-des-clauses-et-conditions-uniformisees-d-achat) (<https://achatsetventes.gc.ca/politiques-et-lignes-directrices/guide-des-clauses-et-conditions-uniformisees-d-achat>) publié par Travaux publics et Services gouvernementaux Canada.

7.2.1 Conditions générales

[2035](#) (2022-12-01), Conditions générales – besoins plus complexes de services s'appliquent au contrat et en font partie intégrante.

7.2.2 Conditions générales supplémentaires

[4 010](#) (2022-12-01), Services : besoins plus complexes, s'appliquent au contrat et en fait partie intégrante.

7.3 Exigences relatives à la sécurité

7.3.1 Les exigences relatives à la sécurité suivantes (LVERS et clauses connexes, comme prévues par le Programme de sécurité des contrats) s'appliquent et font partie intégrante du contrat.

7.3.2 L'entrepreneur doit détenir en permanence, pendant l'exécution du contrat, une attestation de vérification d'organisation désignée (VOD) en vigueur, délivrée par le Programme de sécurité des contrats (PSC), Travaux publics et Services gouvernementaux Canada (TPSGC).

7.3.3 Les membres du personnel de l'entrepreneur devant avoir accès à des établissements dont l'accès est réglementé doivent TOUS détenir une cote de FIABILITÉ en vigueur, délivrée ou approuvée par le PSC, TPSGC.

7.3.4 Les contrats de sous-traitance comportant des exigences relatives à la sécurité NE doivent PAS être attribués sans l'autorisation écrite préalable du PSC, TPSGC.

7.3.5 L'entrepreneur doit respecter les dispositions suivantes :

7.3.5.1 Liste de vérification des exigences relatives à la sécurité et directive de sécurité (s'il y a lieu), reproduite ci-joint à l'annexe C;

7.3.5.2 Manuel de la sécurité des contrats (dernière édition)

7.4 Durée du contrat

7.4.1 Période du contrat

La période du contrat s'étend de la date d'attribution du contrat au 31 octobre 2023 inclusivement.

7.4.2 Option de prolongation du contrat

L'entrepreneur accorde au Canada l'option irrévocable de prolonger la durée du contrat pour un maximum d'une (1) période supplémentaire d'une (1) année chacune, selon les mêmes conditions. L'entrepreneur convient que, pendant la période prolongée du contrat, il sera payé conformément aux dispositions applicables prévues à la Base de paiement.

Le Canada peut exercer cette option à tout moment en envoyant un avis écrit à l'entrepreneur au moins quinze (15) jours civils avant la date d'expiration du contrat. Cette option ne pourra être exercée que par l'autorité contractante et sera attestée, à des fins administratives uniquement, par une modification au contrat.

7.5 Responsables

7.5.1 Autorité contractante

L'autorité contractante pour le contrat est :

Nom : _____
Titre : _____
Direction générale des approvisionnements
Direction : _____
Adresse : _____
Téléphone : ____-____-_____
Adresse de courriel : _____

L'autorité contractante est responsable de la gestion du contrat et toute modification du contrat doit être autorisée par écrit par l'autorité contractante. L'entrepreneur ne doit pas effectuer de travaux dépassant ou sortant du cadre du Contrat en fonction de demandes ou d'instructions verbales ou écrites émanant d'une personne autre que l'autorité contractante.

7.5.2 Chargé de projet

Le chargé de projet pour le contrat est :

Nom : _____
Titre : _____
Organisation : _____
Adresse : _____
Téléphone : ____-____-_____
Adresse de courriel : _____

Le chargé de projet représente le ministère ou l'organisme pour lequel les travaux sont exécutés dans le cadre du contrat. Il est responsable de toutes les questions liées au contenu technique des travaux prévus dans le Contrat. On peut discuter des questions techniques avec le chargé de projet; cependant, celui-ci ne peut pas autoriser les changements à apporter à l'énoncé des travaux. De tels changements peuvent être effectués uniquement au moyen d'une modification au Contrat émise par l'autorité contractante

7.5.3 Représentant de l'entrepreneur

Nom : _____
Titre : _____
Organisation : _____
Adresse : _____
Téléphone : ____-____-_____
Adresse de courriel : _____

7.6 Divulgence proactive des marchés conclus avec d'anciens fonctionnaires

En fournissant des renseignements sur son statut en tant qu'ancien fonctionnaire touchant une pension en vertu de la [Loi sur la pension de la fonction publique](#) (LPFP), l'entrepreneur a accepté que cette information soit publiée sur les sites Web des ministères, dans le cadre des rapports de divulgation proactive des marchés, et ce, conformément à l'[Avis sur la Politique des marchés : 2019-01](#) du Secrétariat du Conseil du Trésor du Canada.

7.7 Paiement

7.7.1 Base de paiement

Honoraires professionnels

À condition de remplir de façon satisfaisante toutes ses obligations en vertu du contrat, l'entrepreneur sera payé un prix ferme dans « l'annexe B », selon un montant total de _____ \$ (*insérer le montant au moment de l'attribution du contrat*). Les droits de douane sont inclus et les taxes applicables sont en sus.

Autres coûts directs

L'entrepreneur sera remboursé pour les coûts directs raisonnablement et convenablement encourus dans le cadre de l'exécution des travaux. Ces coûts seront remboursés au coût réel sans majoration, sur présentation d'un état détaillé accompagné des reçus appropriés.

Coût estimatif : _____ \$

Prix estimatif total du contrat : _____, Taxes applicables en sus.

Option de prolongation du contrat

Pendant la période de prolongation du contrat, l'entrepreneur recevra le prix ferme de _____ \$ (*insérer le montant lors de l'attribution du contrat*) pour exécuter tous les travaux liés à la prolongation du contrat.

7.7.2 Limite des dépenses

La responsabilité totale du Canada envers l'entrepreneur en vertu du contrat ne doit pas dépasser la somme de _____ \$. Les droits de douane sont inclus et les taxes applicables sont en sus.

Aucune augmentation de la responsabilité totale du Canada ou du prix des travaux découlant de tout changement de conception, de toute modification ou interprétation des travaux, ne sera autorisée ou payée à l'entrepreneur, à moins que ces changements de conception, modifications ou interprétations n'aient été approuvés, par écrit, par l'autorité contractante avant d'être intégrés aux travaux. L'entrepreneur n'est pas tenu d'exécuter des travaux ou de fournir des services qui entraîneraient un dépassement de la responsabilité totale du Canada avant d'obtenir l'autorisation écrite de l'autorité contractante. L'entrepreneur doit informer, par écrit, l'autorité contractante de la suffisance de cette

somme :

- (a) lorsque 75 % de la somme est engagée, ou
- (b) quatre mois avant la date d'expiration du contrat, ou
- (c) dès que l'entrepreneur juge que les fonds du contrat sont insuffisants pour l'achèvement des travaux,

selon la première de ces conditions à se présenter.

Lorsqu'il informe l'autorité contractante que les fonds du contrat sont insuffisants, l'entrepreneur doit lui fournir par écrit une estimation des fonds additionnels nécessaires. La présentation de cette information par l'entrepreneur n'augmente pas la responsabilité du Canada.

7.7.3 Paiement unique H1000C (12-05-2008)

Le Canada paiera l'entrepreneur lorsque les travaux seront terminés et livrés conformément aux dispositions de paiement du contrat si :

- (a) une facture exacte et complète ainsi que tout autre document exigé par le contrat ont été soumis conformément aux instructions de facturation prévues au contrat;
- (b) tous ces documents ont été vérifiés par le Canada;
- (c) les travaux livrés ont été acceptés par le Canada.

7.7.4 Vérification discrétionnaire

Le profit estimatif compris dans l'attestation de prix ou de taux fournie par l'entrepreneur peut faire l'objet d'une vérification des comptes par le Canada, avant ou après que l'entrepreneur n'a été payé conformément aux conditions du contrat. La vérification des comptes a pour but de déterminer si le profit réel réalisé à la suite d'un seul contrat, s'il en existe un seul, ou si le profit global réel réalisé par l'entrepreneur à la suite d'un ensemble de contrats négociés à prix ferme et à taux fixes basés sur le temps exécutés pendant une période précise et choisie, est raisonnable et justifié par rapport au profit estimatif indiqué dans une ou des attestations de prix ou de taux antérieurs.

Si la vérification démontre que le profit réel n'est pas raisonnable et justifié, comme défini ci-dessus, l'entrepreneur doit rembourser au Canada le trop-payé.

7.7.5 Vérification du temps

Le Canada pourra vérifier le temps imputé et l'exactitude du système d'enregistrement du temps de l'entrepreneur, avant ou après avoir payé ce dernier. Dans le cas où on effectue la vérification après le paiement, l'entrepreneur s'engage à rembourser le trop-payé dès que le Canada lui en fera la demande.

7.8 Instructions relatives à la facturation

L'entrepreneur doit soumettre ses factures conformément à l'article intitulé « Présentation des factures » des conditions générales. Les factures ne doivent pas être soumises avant que tous les travaux mentionnés sur la facture soient terminés.

Instruction aux agents de négociation des contrats : Utiliser le paragraphe suivant lorsque les factures doivent être accompagnées de documents à l'appui. Les documents énumérés sont à titre d'exemples seulement et doivent être révisés pour refléter le besoin. Supprimer ce paragraphe si aucun document à l'appui n'est exigé.

Chaque facture doit être appuyée par :

- (a) une copie des feuilles de temps pour corroborer le temps de travail réclamé;
- (b) une copie du document de sortie et de tout autre document tel qu'il est précisé au contrat;

- (c) une copie des factures, reçus, pièces justificatives pour tous les frais directs et pour tous les frais de déplacement et de subsistance;
- (d) une copie du rapport mensuel sur l'avancement des travaux.

Les factures doivent être distribuées comme suit :

- (a) L'original et un (1) exemplaire doivent être envoyés à l'adresse qui apparaît à la page 1 du Contrat pour attestation et paiement.

7.9 Attestations et renseignements supplémentaires

7.9.1 Conformité

À moins d'indication contraire, le respect continu des attestations fournies par l'entrepreneur avec sa soumission ou préalablement à l'attribution du contrat, ainsi que la coopération constante quant aux renseignements supplémentaires, sont des conditions du contrat et leur non-respect constituera un manquement de la part de l'entrepreneur. Les attestations pourront faire l'objet de vérifications par le Canada pendant toute la durée du contrat.

7.10 Lois applicables

Le contrat doit être interprété et régi selon les lois en vigueur Ontario et les relations entre les parties seront déterminées par ces lois.

7.11 Ordre de priorité des documents

En cas d'incompatibilité entre le libellé des textes énumérés dans la liste, c'est le libellé du document qui apparaît en premier sur la liste qui l'emporte sur celui de tout autre document qui figure plus bas sur la liste.

- (a) les articles de la convention;
- (b) les conditions générales supplémentaires [4010](#) 2022-12-01 Services : besoins plus complexes;
- (c) les conditions générales [2035](#) 2022-12-01, Conditions générales – Besoins plus complexes de services;
- (d) Annexe A, Énoncé des travaux;
- (e) Annexe B, Base de paiement;
- (f) Annexe C, Liste de vérification des exigences relatives à la sécurité;
- (g) la soumission de l'entrepreneur datée le _____,

7.12 Règlement des différends

- (a) Les parties conviennent de maintenir une communication ouverte et honnête concernant les travaux pendant toute leur durée et après.
- (b) Les parties conviennent de se consulter et de collaborer dans l'exécution du contrat, d'informer rapidement toute autre partie des problèmes ou des différends qui peuvent survenir et de tenter de les résoudre.
- (c) Si les parties n'arrivent pas à résoudre un différend au moyen de la consultation et de la collaboration, les parties conviennent de consulter un tiers neutre offrant des services de règlement extrajudiciaire des différends pour tenter de régler le problème.
- (d) Vous trouverez des choix de services de règlement extrajudiciaire des différends sur le site Web Achats et ventes du Canada sous le titre « [Règlement des différends](#) ».

ANNEXE A : ÉNONCÉ DES TRAVAUX

1.0 CONTEXTE

- 1.1 L'Académie canadienne de la défense (ACD) est une direction générale du ministère de la Défense nationale (MDN) et des Forces armées canadiennes (FAC) chargée de la prestation de l'éducation militaire professionnelle. Le Collège militaire royal (CMR) du Canada est une sous-organisation de l'ACD et est une université provinciale accréditée au niveau du premier cycle et des études supérieures. Le CMR compte environ 3 000 étudiants, enseignants et personnel administratif. Comme d'autres universités provinciales, le CMR a besoin d'un réseau universitaire pour assurer les fonctions suivantes : l'enseignement universitaire, la recherche au niveau du premier cycle et des études supérieures, ainsi que la fonction du registraire. De plus amples renseignements sur le réseau du Collège militaire royal (RMC Net) se trouvent à l'**annexe 1**.

2.0 OBJECTIF

- 2.1 L'objectif de cet énoncé des travaux est de permettre aux systèmes d'information et de communication (SIC) de l'ACD d'assurer les services d'un spécialiste des tests d'intrusion des réseaux externes (Pentest) de niveau intermédiaire pouvant travailler à distance, dans le cadre de l'arrangement en matière d'approvisionnement en services professionnels en informatique centrés sur les solutions – domaines d'expertise : [10. Gestion de la sécurité PICS SA – Domaines d'expertise – Aperçu du SPICS – Services professionnels – Achat et vente – SPAC \(tpsgc-pwgsc.gc.ca\)](#)

3.0 BESOIN

- 3.1 Les SIC de l'ACD ont besoin d'un spécialiste des tests d'intrusion des réseaux externes de niveau intermédiaire ayant la qualification de Certified Ethical Hacker (CEH) pour effectuer deux (2) pentest. Le premier pentest est un pentest de réseau externe visant à identifier et à exploiter les vulnérabilités de sécurité du réseau et des hôtes au sein des infrastructures en réseau accessibles sur Internet et exploitées par le CMR. Ce pentest doit suivre la méthodologie PTES (norme d'exécution des tests d'intrusion). Le second pentest est une application Web pentest des applications Web accessibles au CMR par l'entremise d'une numération d'applications Web non authentifiées et automatisées qui doivent être conformes à la norme de sécurité des données (DSS) de l'industrie des cartes de paiement (PCI). Les SIC de l'ACD doivent déterminer l'application Web du CMR qui sera ciblée pendant le pentest, qui ne sera pas inférieure à sept (7), mais qui ne dépassera pas un maximum de dix (10) applications Web. Ce pentest doit suivre la méthodologie de l'Open Web Application Security Project (OWAS).
- 3.2 L'entrepreneur pendant le pentest du réseau externe est de :
- 3.2.1 Découverte des dispositifs – L'entrepreneur établira un profil des plages de protocole Internet (IP) fournies par le CMR pour repérer les dispositifs externes actifs, qui ne seront pas inférieurs à dix (10) dispositifs externes actifs, mais qui ne dépasseront pas un maximum de trente-cinq (35) dispositifs externes actifs.
 - 3.2.2 Analyse de la vulnérabilité – L'entrepreneur analysera les services de réseau disponibles et les empreintes de la pile IP de tous les dispositifs externes actifs trouvés lors de la phase de découverte des dispositifs.
 - 3.2.3 Validation des vulnérabilités – L'entrepreneur tentera de valider les résultats de l'analyse des vulnérabilités afin de repérer (et d'ignorer) tout résultat faussement positif et de valider les autres résultats positifs des tests automatisés.
 - 3.2.4 Exploitation – Après avoir compris les rôles des dispositifs externes, les relations de confiance potentielles, les services de réseau accessibles et les vulnérabilités

potentielles, l'entrepreneur tentera d'accéder aux systèmes cibles.

- 3.2.5 Post-exploitation – Après avoir terminé la phase d'exploitation et obtenu l'accès à tous les hôtes et données vulnérables, l'entrepreneur tentera d'augmenter les privilèges sur tous les hôtes exploités. L'entrepreneur tentera de tirer parti de cet accès et d'accéder aux données (telles que le hachage des mots de passe et les jetons d'authentification) sur ces hôtes pour obtenir un accès supplémentaire au réseau du CMR et tenter d'accéder à d'autres systèmes et données.

3.1 L'entrepreneur pendant le pentest de l'application Web est de :

- 3.3.1 Contournement de la validation des entrées – L'entrepreneur supprimera les routines de validation côté client et les restrictions de vérification des limites pour confirmer que les contrôles sont mis en œuvre sur les paramètres d'application envoyés au serveur.
- 3.3.2 Injection SQL – L'entrepreneur soumettra des commandes SQL spécialement conçues dans les champs de saisie pour valider les contrôles de saisie mis en place pour la protection des données de la base de données.
- 3.3.3 Scriptes entre sites – L'entrepreneur soumettra un contenu actif à l'application dans le but d'amener le navigateur Web d'un utilisateur à exécuter un code non autorisé et non filtré. Ce test est destiné à valider les contrôles d'entrée de l'utilisateur.
- 3.3.4 Altération des paramètres – L'entrepreneur modifiera les chaînes d'interrogation, les paramètres et les champs cachés dans le but d'obtenir un accès non autorisé aux données d'utilisateur ou aux fonctionnalités de l'application.
- 3.3.5 Navigation forcée – L'entrepreneur énumérera les fichiers situés sur un serveur Web pour tenter d'accéder à des fichiers et à des données d'utilisateur qui ne sont pas explicitement montrés à l'utilisateur dans l'interface de l'application.
- 3.3.6 Portes dérobées et options de débogage – L'entrepreneur repérera le code laissé par les concepteurs à des fins de débogage qui pourrait permettre à un intrus d'obtenir des niveaux d'accès supplémentaires.
- 3.3.7 Subversion de la configuration – L'entrepreneur évaluera les serveurs Web et les serveurs d'application du CMR pour détecter les configurations incorrectes qui pourraient créer des vecteurs d'attaque.

4.0 LIEU DE TRAVAIL

- 4.1 Tous les travaux doivent être effectués à distance et toutes les réunions se dérouleront virtuellement.

5.0 EXIGENCES LINGUISTIQUES

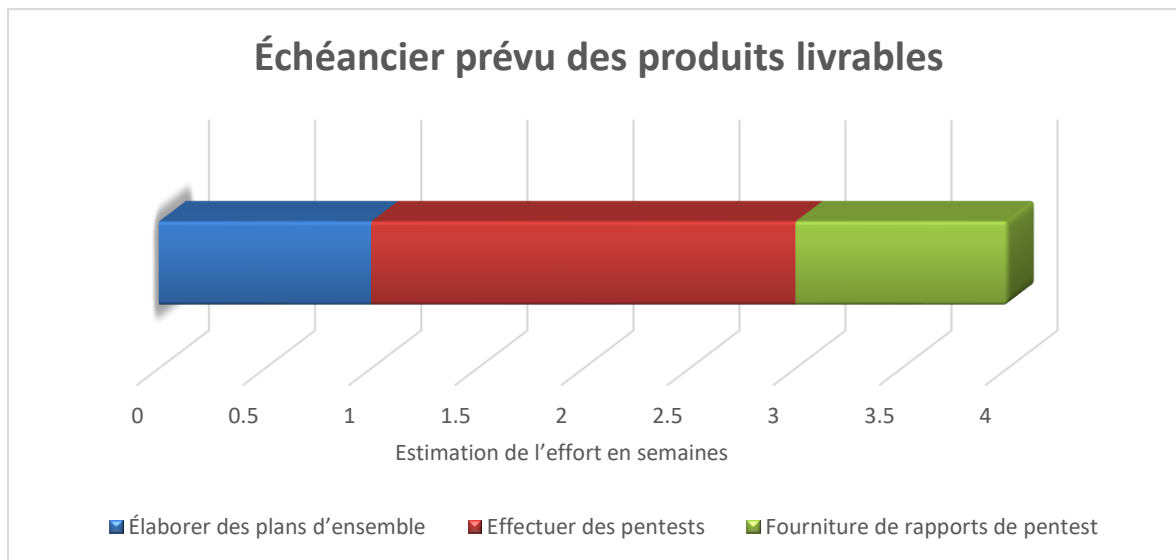
- 5.1 L'interaction se fera en anglais.

6.0 TÂCHES ET PRODUITS LIVRABLES

6.1 Tâches

- 6.1.1 La ressource d'entrepreneur doit réaliser un pentest du réseau externe sur le réseau du CMR,

- 6.1.2 La ressource d'entrepreneur doit fournir un aperçu du plan de test de réseau externe suivant la méthodologie PTES et le faire approuver par SIC de l'ACD.
 - 6.1.3 Ressource d'entrepreneur doit réaliser le pentest du réseau externe conformément au plan d'ensemble après approuver par SIC de l'ACD.
 - 6.1.4 La ressource d'entrepreneur doit réaliser un pentest d'application Web sur les applications Web du CMR après approbation du plan directeur par SIC de l'ACD.
 - 6.1.5 La ressource d'entrepreneur doit fournir le plan d'ensemble d'un pentest d'application Web suivant la méthodologie OWASP.
 - 6.1.5 La ressource d'entrepreneur doit réaliser le pentest de l'application Web conformément au plan d'ensemble après approuver par SIC de l'ACD.
 - 6.1.6 La ressource d'entrepreneur doit continuellement documenter la liste des vulnérabilités prioritaires, les méthodes pour les exploiter, les mesures correctives recommandées adaptées à l'environnement du CMR tout au long de la période du contrat.
 - 6.1.7 La ressource d'entrepreneur doit fournir au minimum un rapport écrit hebdomadaire aux SIC de l'ACD.
- 7.2 Produits livrables
- 7.2.1 L'entrepreneur doit documenter et fournir un plan d'ensemble de chaque pentest dans un format compatible avec les applications MS Office aux SIC de l'ACD, et fournir une consultation du plan d'ensemble aux SIC de l'ACD avant le début du pentest; le temps d'effort estimé requis est d'une semaine. L'**annexe 3** contient un modèle de rapport hebdomadaire sur l'avancement des tests d'intrusion
 - 7.2.2 L'entrepreneur doit effectuer un pentest du réseau externe sur le réseau du CMR, ainsi qu'un pentest d'application Web sur l'application Web du CMR. Le temps d'effort requis est estimé à deux semaines.
 - 7.2.3 L'entrepreneur doit fournir au moins les documents suivants dans le rapport du pentest (mais pas limité a):
 - a. Sommaire;
 - b. détails techniques des vulnérabilités;
 - c. méthodologies des tests;
 - d. correctifs et recommandations; et
 - e. niveau de risque.



9.0 RESPONSABILITÉS DU MDN

9.1 Le MDN fournira les éléments suivants à l'entrepreneur :

9.1.1 Consultation technique en temps opportun et approbations dans les 24 heures de la part des SIC de l'ACD.

10.0 RESPONSABILITÉS DE L'ENTREPRENEUR

10.1 L'entrepreneur doit fournir tous les biens de TI et de télécommunication nécessaires pour produire les produits livrables et participer aux réunions virtuelles.



Appendice 1 à l'annexe D : Réseau du Collège militaire royal (RMC Net)

1.0 Contexte

- 1.1 Les environnements universitaires modernes reposent sur un mélange dynamique d'infrastructures informatiques et de services réseau pour faciliter la mission fondamentale de l'institution. Par exemple, l'enseignement en classe/en laboratoire dans des espaces d'information, des espaces d'apprentissage pour l'étude individuelle et en petits groupes et l'interaction, l'organisation d'ateliers et de symposiums académiques, des réunions ad hoc entre chercheurs universitaires et comités administratifs, etc. Il y a des ordinateurs de laboratoire fixes et des postes de travail de bureau sur le campus du Collège militaire royal (CMR) qui fournissent des outils normalisés de productivité de bureau, l'accès aux bases de données et aux outils administratifs du CMR, ainsi que des logiciels spécialisés de laboratoire et d'analyse.
- 1.2 L'environnement universitaire contemporain, ainsi que celui de l'avenir prévisible, dépend d'un accès omniprésent à l'information en ligne. À bien des égards, l'accès en ligne au Web mondial est aussi important pour une université contemporaine que sa bibliothèque. La disponibilité de l'information en ligne est fondamentale pour l'interaction dynamique ad hoc des étudiants, des enseignants, du personnel et des chercheurs.
- 1.3 Il existe une grande variété d'outils de collaboration axés sur la technologie qui offrent un éventail d'expériences de collaboration. Les outils que l'on trouve dans les systèmes de gestion de l'apprentissage dédiés existants ont été élaborés plus particulièrement pour soutenir l'environnement universitaire; ces outils fournissent, par leur conception, la structure nécessaire pour soutenir l'apprentissage universitaire.

2.0 Réseau du Collège militaire royal (RMC Net)

- 2.1 Le réseau du Collège militaire royal (RMC Net) est un réseau indépendant accessible par Internet qui sert d'outil principal d'enseignement et d'administration académique pour les fonctions universitaires du Collège militaire royal (CMR). Le réseau offre un large éventail de services accessibles sur Internet, car les étudiants du CMR, tant au premier cycle qu'aux cycles supérieurs, fonctionnent principalement dans l'espace. Apportez votre propre appareil (AVPA). Les applications du réseau comprennent à la fois le système de gestion de l'apprentissage du CMR (basé sur Moodle) et le système d'information des étudiants (applications sur mesure basées sur Oracle) tout en soutenant les fonctions complètes du registraire de l'université, y compris les admissions, les horaires et les droits de scolarité des étudiants payants. Le réseau fonctionne au niveau Protégé A tout en détenant des renseignements Protégé B, y compris les numéros d'assurance sociale, pour générer des relevés d'impôts. RMC Net est structuré selon le

modèle à niveaux de Microsoft pour la gestion de l'accès privilégié (GAP), qui crée des niveaux distincts de comptes d'administrateur ainsi que la mise en œuvre de la solution de mot de passe d'administrateur local (LAPS) de Microsoft pour empêcher l'escalade des privilèges et protéger l'accès aux services de niveau 0 et de niveau 1.

- 2.2 RMC Net est géré à la fois par l'équipe des systèmes d'information sur ordinateur de l'Académie canadienne de la défense (SIC de l'ACD) et par Services partagés Canada (SPC). L'équipe du réseau local (LAN) du SSC Kingston est responsable des opérations de la connexion du réseau étendu (WAN) du CMR à l'Internet par l'intermédiaire des connexions ORION et Bell, du pare-feu du RMC Net et du LAN du RMC Net. Les SCI de l'ACD sont responsables du fonctionnement des serveurs, de la gestion des applications et du soutien informatique.

3.0 Environnement administratif du CMR

- 3.1 Le bureau du registraire participe à un large éventail de fonctions administratives, comme le recrutement, l'admission, le soutien aux programmes de premier cycle et d'études supérieures, la gouvernance et l'évaluation et la reconnaissance des acquis (ERA).

4.0 Recrutement/Admissions

- 4.1 Le bureau du registraire est le premier point de contact pour les étudiants potentiels, ce qui commence par recruter les étudiants potentiels. Du point de vue des ressources informatiques, le CMR gère des sites Web externes. Le public de ces sites Web comprendra d'autres universitaires en dehors des collèges qui chercheront à établir des contacts de recherche.
- 4.2 Le bureau du registraire utilise un certain nombre d'applications commerciales et sur mesure pour assurer l'administration du collège :

- 4.2.1 Les détails de tous les étudiants inscrits au CMR et au CMR-SJ sont conservés dans une application appelée CISA qui est utilisée par le personnel du registraire et d'autres personnes jouant un rôle dans la gestion et l'administration des étudiants.
- 4.2.2 L'établissement et la mise à jour des horaires de cours relèvent également de la compétence du bureau du registraire. La planification tient compte de toutes les ressources pédagogiques et des horaires des étudiants et du personnel. L'une des principales exigences de la capacité de planification est la « souplesse »; les horaires doivent être dynamiques afin de répondre aux exigences changeantes de nombreux points de vue différents, p. ex., étudiants, personnel, disponibilité des ressources, TI, etc.
- 4.2.3 L'outil « Degree Navigator » est mis à la disposition des étudiants et du personnel afin de faciliter le suivi des progrès réalisés en vue de l'obtention d'un diplôme.
- 4.2.4 L'admission des étudiants est coordonnée entre le Collège et le Groupe de recrutement des Forces canadiennes (GRFC); la liaison entre les deux organisations se fait par l'intermédiaire du logiciel CFRIMS installé sur le réseau DWAN Enterprise. Une fois l'étudiant inscrit, tous les détails importants sont transférés vers l'outil interne CISA.
- 4.2.5 Lorsque les étudiants paient pour leurs études, des exigences provinciales et fédérales liées au RAFEO et à l'impôt exigent que les étudiants conservent l'accès à leur dossier après l'obtention de leur diplôme afin de préparer des présentations aux autorités compétentes, p. ex., les étudiants peuvent devoir soumettre un formulaire T2200 lorsqu'ils préparent leur déclaration de revenus après l'obtention de leur diplôme.
- 4.2.6 Le Collège a l'obligation légale de prendre des mesures d'adaptation pour les étudiants handicapés afin de maximiser leurs chances de réussite. Ces aménagements peuvent

nécessiter l'installation et l'utilisation par les étudiants de logiciels spécialisés supplémentaires dans un délai relativement court.

- 4.3 L'application CISA, du fait qu'elle contient des données à caractère personnel, contient des renseignements considérés comme « désignés ». Ces renseignements doivent être gérés conformément aux politiques de sécurité pertinentes du gouvernement du Canada en matière de protection des renseignements personnels et de sécurité, tout en respectant les exigences en matière de rapports du Programme d'analyse de la défense.

5.0 Recherche

- 5.1 La recherche fait partie intégrante des études supérieures. La recherche universitaire est le fondement de l'enseignement, tant au niveau du premier que des études supérieures. L'environnement de recherche est constitué de professeurs, d'étudiants diplômés, de boursiers postdoctoraux, d'assistants de recherche et de chercheurs invités; la recherche est entreprise par des groupes partageant un objectif de recherche commun, et les résultats de cette recherche sont rédigés de manière rigoureuse sur le plan académique, pour être diffusés au sein de l'institution.
- 5.2 La recherche effectuée au CMR s'harmonise largement sur les priorités des FAC, mais la liberté universitaire est garantie aux membres du corps professoral pour entreprendre des recherches comme ils l'entendent. Cette liberté comprend non seulement les sujets particuliers de recherche, mais également l'accès libre et sans entraves à d'autres réseaux et aux outils et techniques utilisés par les chercheurs dans le développement des connaissances. Du point de vue des ressources informatiques, cette liberté comprend les outils informatiques utilisés pour l'analyse et la simulation, ainsi que toute instrumentation particulière éventuellement nécessaire; dans le cas d'instruments spécialisés, ceux-ci sont souvent élaborés en externe par des fabricants spécialisés; en outre, le fabricant peut exiger un accès à distance à l'instrument pour en assurer l'entretien et les mises à jour, à mesure que l'instrument évolue parallèlement à la recherche.
- 5.3 Le passage aux formats numériques pour le stockage des renseignements a un certain nombre d'incidences conséquentes;
- 5.3.1 les formats multimédias diffusés en continu doivent pouvoir être consultés à partir d'un large éventail de sources publiques et fiables;
 - 5.3.2 les présentations sont devenues des sources d'information riches et stratifiées qui intègrent des éléments visuels et des ensembles de données complexes;
 - 5.3.3 des fonctions analytiques et statistiques sont également intégrées dans les logiciels évolutifs utilisés dans l'enseignement et la recherche.

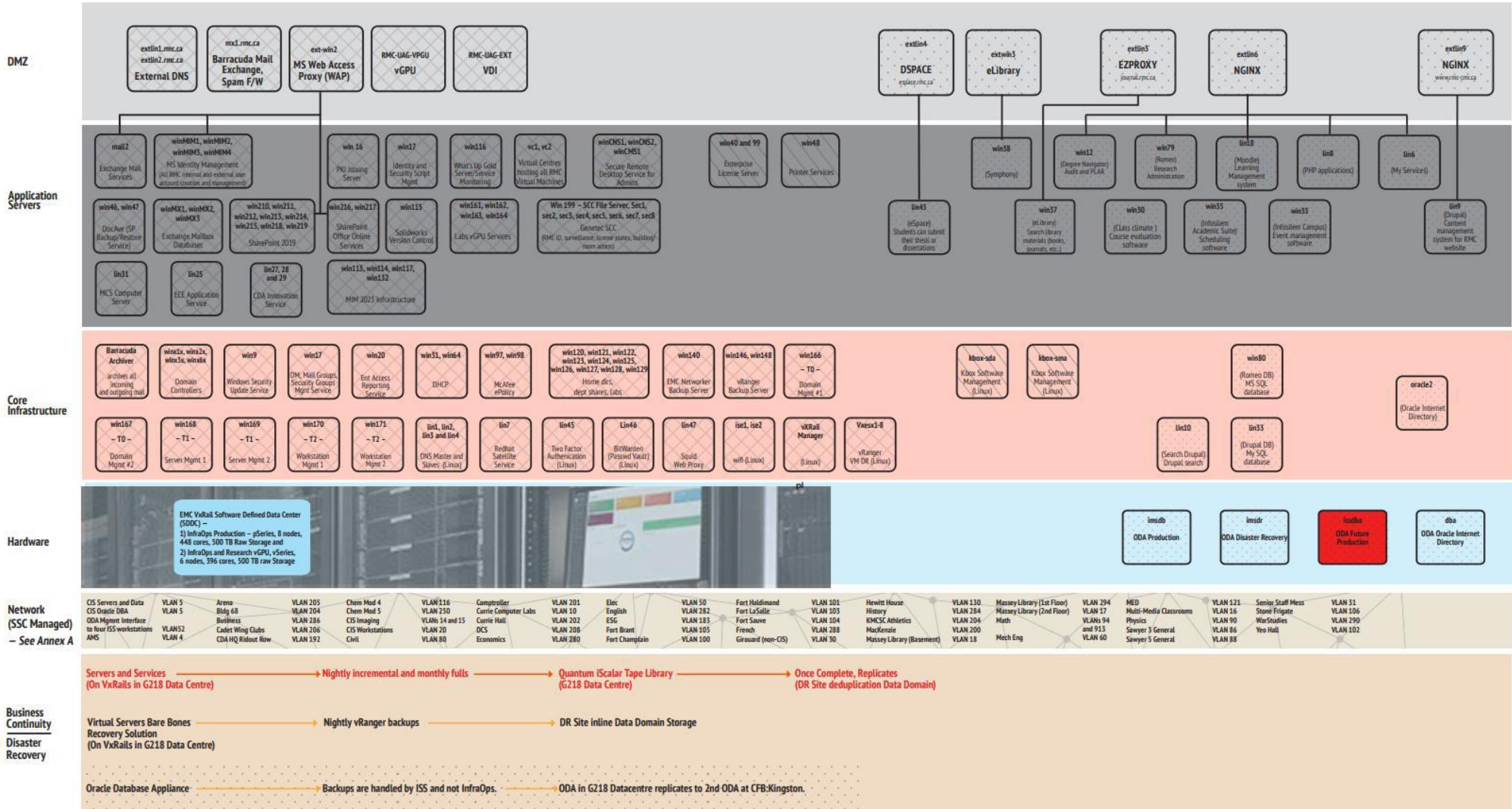
6.0 Sécurité et vie privée

- 6.1 Les exigences relatives à la sécurité des renseignements et à la protection de la vie privée semblent contredire les exigences relatives à l'accès sans fil, au BYOD, à l'agilité, à la souplesse, à l'accès libre/non filtré à l'Internet et à l'accès au réseau par des organismes externes ne relevant pas de la portée des autorisations du gouvernement du Canada. Afin de répondre aux exigences nécessaires en matière de sécurité et de confidentialité, RMC Net a été structuré à l'aide du modèle de niveau de Microsoft pour la GAP, et Microsoft LAPS a été mis en œuvre.

RMCnet Infrastructure, Servers and Services

FIREWALL – SSC MANAGED

- Core infrastructure Services – Fully maintained by InfraOps
- Kingston Site Team Section
- Information Solution Services (Servers maintained by InfraOps, Apps maintained by ISS)



Appendice 2 à l'annexe A : L'application Web du réseau du CMR va faire l'objet d'un test d'intrusion

Les sites Internet et intranet suivants entrent dans le champ d'application du test d'intrusion de l'application Web :

services.rmc.ca (obligatoire)

Moodle.rmc.ca (obligatoire)

espace.rmc.ca

elibrary.rmc.ca

journal.rmc.ca

normes.rmc.ca

romeo.rmc.ca

dept.rmc.ca

collab.rmc.ca

www.rmc-cmr.ca (obligatoire)

ANNEXE B : BASE DE PAIEMENT

Le total ne doit pas dépasser _____ \$ (taxes applicables en sus) pour les services décrits dans l'Énoncé des travaux (annexe A). Le paiement sera effectué sur présentation d'une facture approuvée.

Produits livrables	Coût par heure	Niveau d'effort (heures)	Coût étendu
Deux (2) tests externes d'intrusion du réseau (Pentests)	___/h	160 heures	
Sous-total :			
Taxes (TVH) :			
Total à ne pas dépasser :			

Période facultative :

Produits livrables	Coût par heure	Niveau d'effort (heures)	Coût étendu
Travaux supplémentaires de test d'intrusion de réseau externe	___/h	80 heures	
Sous-total :			
Taxes (TVH) :			
Total à ne pas dépasser :			

Solicitation No. - N° de l'invitation

W4938-23-073S

Client Ref. No. - N° de réf. du client

Amd. No. - N° de la modif.

File No. - N° du dossier

Buyer ID - Id de l'acheteur

Wood.JMS

CCC No./N° CCC - FMS No./N° VME

**ANNEXE C : LISTE DE VÉRIFICATION DES EXIGENCES RELATIVES À LA SÉCURITÉ
(VOIR CI-JOINT)**