Public Works and Government Services Canada | Travaux publics et Services gouvernementaux Canada

RETURN BIDS TO:
RETOURNER LES SOUMISSIONS À:

Bid Receiving - PWGSC / Réception des soumissions - TPSGC
11 Laurier St. / 11, rue Laurier
Place du Portage , Phase III
Core 0B2 / Noyau 0B2
Gatineau, Québec K1A 0S5
Bid Fax: (819) 997-9776

REQUEST FOR PROPOSAL
DEMANDE DE PROPOSITION

Proposal To: Public Works and Government Services Canada

We hereby offer to sell to Her Majesty the Queen in right of Canada, in accordance with the terms and conditions set out herein, referred to herein or attached hereto, the goods, services, and construction listed herein and on any attached sheets at the price(s) set out therefor.

Proposition aux: Travaux Publics et Services Gouvernementaux Canada

Nous offrons par la présente de vendre à Sa Majesté la Reine du chef du Canada, aux conditions énoncées ou incluses par référence dans la présente et aux annexes ci-jointes, les biens, services et construction énumérés ici sur toute feuille ci-annexée, au(x) prix indiqué(s).

Comments - Commentaires

There are security requirements associated with this requirement, consult Part 6 and Part 7.

Ce besoin comporte des exigences relatives à la sécurité, consulter la Partie 6 et la Partie 7.

Vendor/Firm Name and Address
Raison sociale et adresse du fournisseur/de l'entrepreneur

Issuing Office - Bureau de distribution

Training and Specialized Services Division/Division de la formation et des services spécialisés
Terrasses de la Chaudière 5th Floo
Terrasses de la Chaudière 5e étage
10 Wellington Street,
10, rue Wellington,
Gatineau
Québec
K1A 0S5

Title - Sujet Outil d'évaluation et la formation
Outil d'évaluation et la formation de PP

Solicitation No. - N° de l'invitation	**Date**
W4938-21330S/A	2021-06-09

Client Reference No. - N° de référence du client
W4938-21330S

GETS Reference No. - N° de référence de SEAG
PW-$$ZH-113-39633

File No. - N° de dossier	**CCC No./N° CCC - FMS No./N° VME**
113zh.W4938-21330S	

Solicitation Closes - L'invitation prend fin

at - à 02:00 PM Eastern Daylight Saving Time EDT
on - le 2021-07-20 Heure Avancée de l'Est HAE

F.O.B. - F.A.B. Specified Herein - Précisé dans les présentes
Plant-Usine: ☐ **Destination:** ☐ **Other-Autre:** ☑

Address Enquiries to: - Adresser toutes questions à:	**Buyer Id - Id de l'acheteur**
Reynolds(zh), Diane	113zh

Telephone No. - N° de téléphone	**FAX No. - N° de FAX**
(613) 858-8571 ( )	( ) -

Destination - of Goods, Services, and Construction:
Destination - des biens, services et construction:
See Herein

Voir aux présentes

Instructions: See Herein

Instructions: Voir aux présentes

Delivery Required - Livraison exigée	**Delivery Offered - Livraison proposée**
See Herein – Voir ci-inclus	

Vendor/Firm Name and Address
Raison sociale et adresse du fournisseur/de l'entrepreneur

Telephone No. - N° de téléphone
Facsimile No. - N° de télécopieur

Name and title of person authorized to sign on behalf of Vendor/Firm (type or print)
Nom et titre de la personne autorisée à signer au nom du fournisseur/ de l'entrepreneur (taper ou écrire en caractères d'imprimerie)

Signature **Date**

Canada

TITRE

Demande de soumissions # W3802-210054/A pour la prestation des services professionnels suivants : développer un outil d'évaluation des cyberopérateurs; évaluer les stagiaires utilisant le outil d'évaluation, et développer la formation de perfectionnement professionnel des cyberopérateurs.

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, clauses et conditions relatives à la demande de soumissions;

Partie 3 Instructions pour la préparation des soumissions : 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 des renseignements supplémentaires à fournir;

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

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

Les pièces jointes comprennent le barème de prix, les critères techniques, et les attestations et renseignements supplémentaires.

Les annexes comprennent l'énoncé des travaux, la liste de vérification des exigences relatives à la sécurité et l'entente de non-divulgation.

1.2 Sommaire

Le ministère de la Défense nationale requiert un entrepreneur qui à développer et livrer un outil d'évaluation des cyberopérateurs par rapport au matériel de cours de qualification du grade de soldat, à évaluer les stagiaires utilisant le outil d'évaluation, et à développer et livre une trousse de formation de perfectionnement professionnel correspondant au matériel de cours de qualification du grade de soldat. Pour le livrer de la formation de perfectionnement professionnel des cyberopérateurs aux stagiaires, l'entrepreneur doit fournir un centre de formation et des installations situés dans les limites géographiques de Kingston (Ontario) ou la Région de la Capitale nationale.

La période du contrat est à partir de la date de signature du contrat jusqu'au 31 décembre 2022 inclusivement.

Ce besoin est assujetti aux dispositions de l'Accord de partenariat transpacifique global et progressiste (PTPGP), et de l'Accord de libre-échange canadien (ALEC).

Ce besoin comporte des exigences relatives à la sécurité. Pour plus de renseignements, consulter la Partie 6 et la Partie 7.

Le contrat subséquent ne doit pas être utilisé pour les livraisons à effectuer dans une région visée par une entente de revendication territoriale globale.

Cette demande de soumissions permet aux soumissionnaires d'utiliser le service Connexion postel offert par la Société canadienne des postes pour la transmission électronique de leur soumission. Les soumissionnaires doivent consulter la partie 2, Instructions à l'intention des soumissionnaires, et partie 3, Instructions pour la préparation des soumissions, de la demande de soumissions, pour obtenir de plus amples renseignements.

1.3 Compte rendu

Les soumissionnaires peuvent demander un compte rendu des résultats du processus de demande de soumissions. Les soumissionnaires devraient en faire la demande à l'autorité contractante dans les 15 jours ouvrables suivant la réception des résultats du processus de la demande de soumissions. Le compte rendu peut être fourni par écit, par téléphone ou en personne.

PARTIE 2 - INSTRUCTIONS À L'INTENTION DES SOUMISSIONNAIRES

2.1 Instructions, clauses et conditions uniformisées

Toutes les instructions, clauses et conditions identifiées dans la demande de soumissions par un numéro, une date et un titre sont reproduites dans le Guide des clauses et conditions uniformisées d'achat (CCUA) (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 s'engagent à respecter les instructions, les clauses et les conditions de la demande de soumissions, et acceptent les clauses et les conditions du contrat subséquent.

Le document 2003 (2020-05-28), Instructions uniformisées - biens ou services - besoins concurrentiels, est incorporé par renvoi dans la demande de soumissions et en fait partie intégrante.

Le paragraphe 4 de l'article 5, Présentation des soumissions, des Instructions uniformisées 2003 incorporées ci-haut par renvoi, est modifié comme suit :

Supprimer : 60 jours
Insérer : 120 jours civils.

2.2 Présentation des soumissions

Les soumissions doivent être présentées uniquement à l'Unité de réception des soumissions de TPSGC par l'entremise du service Connexion postel au plus tard à la date et à l'heure indiquées sur la page 1 de la demande de soumissions.

Pour les soumissionnaires qui doivent s'inscrire au service Connexion postel, l'adresse courriel à utiliser est : tpsgc.dgareceptiondessoumissions-abbidreceiving.pwgsc@tpsgc-pwgsc.gc.ca.

Les soumissionnaires intéressés doivent s'inscrire quelques jours avant la date de clôture de la demande de soumissions.

Les soumissions ne seront pas acceptées si elles sont envoyées directement à cette adresse courriel. Cette adresse courriel doit être utilisée pour ouvrir une conversation Connexion postel, tel qu'il est indiqué dans les Instructions uniformisées 2003 ou pour envoyer des soumissions au moyen d'un message Connexion postel si le soumissionnaire utilise sa propre licence d'utilisateur du service Connexion postel.

En raison de la nature de la présente demande de soumissions, TPSGC n'acceptera pas les soumissions qui lui sont transmises par télécopieur ou par courrier électronique.

2.3 Ancien fonctionnaire

Les contrats attribués à des 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 avec des anciens fonctionnaires, les soumissionnaires doivent fournir l'information exigée dans la pièce joint 2 à la Partie 3 avant l'attribution du contrat. Si la réponse aux questions et, s'il y a lieu les renseignements

requis, n’ont pas été fournis avant que l’évaluation des soumissions soit complétée, le Canada informera le soumissionnaire du délai à l’intérieur duquel l’information doit être fournie. Le défaut de se conformer à la demande du Canada et satisfaire à l’exigence dans le délai prescrit rendra la soumission non recevable.

2.4 Lois applicable

Tout contrat subséquent sera interprété et régi selon les lois en vigueur la province de l’Ontario, le Canada, 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 ne 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.

PARTIE 3 - INSTRUCTIONS POUR LA PRÉPARATION DES SOUMISSIONS

3.1 Instructions pour la préparation des soumissions

a) En raison du caractère de la demande de soumissions, les soumissions transmises par télécopieur ou courrier électronique à l'intention de TPSGC ne seront pas acceptées;

b) La soumission doit être séparée comme suit :

Section I : Soumission technique;
Section II : Soumission financière; et
Section III : Attestations et renseignements supplémentaires;

c) Le Canada demande au soumissionnaire de présenter sa soumission électronique en utilisant le système Connexion postel de la Société canadiennes des postes conformément à la section 08 des Instructions uniformisées 2003. Le système Connexion postel a une limite de 1 Go par message individuel affiché et une limite de 20 Go par conversation;

d) Le Canada ne demande pas de copies papier de la soumission; et

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

Section I : soumission technique

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

La soumission technique devrait traiter clairement et de manière suffisamment approfondie des points faisant l'objet des critères d'évaluation en fonction desquels la soumission sera évaluée. Il ne suffit pas de reprendre simplement les énoncés contenus dans la demande de soumissions. Afin de faciliter l'évaluation de la soumission, le Canada demande que les soumissionnaires reprennent les sujets dans l'ordre des critères d'évaluation, sous les mêmes rubriques. Pour éviter les recoupements, les soumissionnaires peuvent faire référence à différentes sections de leur soumission en indiquant le numéro de l'alinéa et de la page où le sujet visé est déjà traité.

La Partie 4, Procédures d'évaluation, comprend d'autres instructions que les soumissionnaires devraient considérer au moment de préparer leur soumission technique.

Section II : soumission financière

a) Les soumissionnaires doivent présenter leur soumission financière en dollars canadiens et en conformité avec le barème de prix détaillé dans la pièce jointe 1 de la Partie 3.

b) Les soumissionnaires doivent soumettre taux FAB destination; les droits de douane et les taxes d'accise canadiens compris, s'il y a lieu; et les taxes applicables exclues.

c) Au moment de préparer leur soumission financière, les soumissionnaires devraient examiner la clause 4.1.3, Évaluation financière, de la Partie 4; et l'article 7.7, Paiement, de la partie 7.

Section III : attestations et renseignements supplémentaires

Les soumissionnaires devraient inclure dans la Section III de leur soumission les attestations exigées à la Partie 5 et, s'il y a lieu, toute documentation connexe et renseignements supplémentaires. Cette demande de soumissions utilise la technologie Format de document portable (PDF). Pour accéder aux formulaires PDF, les soumissionnaires doivent avoir un lecteur PDF installé. Si les soumissionnaires n'ont pas déjà un tel lecteur, il existe de nombreux lecteurs PDF disponibles sur l'Internet. Il est recommandé d'utiliser la plus récente version du lecteur PDF afin de bénéficier de toutes les fonctionnalités des formulaires interactifs.

a) Les soumissionnaires doivent compléter les attestations et fournir les renseignements supplémentaires en utilisant le formulaire PDF à remplir à la pièce jointe 2 de la Partie 3 - Attestations;

b) Les soumissionnaires devrait remplir le formulaire interactif en entier avant de l'imprimer. Les soumissionnaires doivent noter que le fait de simplement imprimer le formulaire avant de le remplir à l'écran pourrait entraîner l'omission de certains champs qui apparaissent au moment de remplir le formulaire électroniquement, ce qui entraînera des attestations incomplètes; et

c) Le formulaire doivent être signé.

PIÈCE JOINTE 1 DE LA PARTIE 3, BARÈME DE PRIX

Le soumissionnaire doit compléter ce barème de prix et l'inclure dans sa soumission financière.

Les données volumétriques comprises dans ce barème de prix sont fournies uniquement aux fins de la détermination du prix évalué de chaque soumission. Elles ne doivent pas être considérées comme une garantie contractuelle. Leur inclusion dans ce barême de prix ne représente pas un engagement de la part du Canada que son utilisation future des services décrits dans la demande de soumissions correspondra à ces données.

Les prix et taux compris dans ce barème de prix comprennent le coût estimatif total de tous les frais de déplacements et de subsistance qui pourraient devoir être engagés pour l'éxécution des travaux décrits à la Partie 7 de la demande de soumissions. Le Canada n'acceptera pas dans le cadre de tout contrat subséquent les dépenses de déplacement et de subsistance que l'entrepreneur pourrait devoir engager pour la réinstallation nécessaire des ressources afin de satisfaire à ses obligations contractuelles.

Si le soumissionnaire ajoute des conditions ou apporte des changements au barème de prix, la soumission financière du soumissionnaire sera déclarée non recevable.

Voir la feuille de calcul « Microsoft excel » ci-jointe, piece-jointe 1 de la partie 3 - barème de prix.xls

PIÈCE JOINTE 2 DE LA PARTIE 3, ATTESTATIONS ET RENSEIGNEMENTS SUPPLÉMENTAIRES

Voir le formulaire PDF remplissable – Pièce-jointe 2 de la partie 3 - Attestations.pdf

PARTIE 4 - PROCÉDURES D'ÉVALUATION ET MÉTHODE DE SÉLECTION

4.1 Procédures d'évaluation

Les soumissions seront évaluées par rapport à l'ensemble des exigences de la demande de soumissions, incluant les critères d'évaluation technique.

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

4.1.1 Processus de conformité des soumissions en phases

4.1.1.1 Généralités

a) Le Canada appliquera le processus de conformité des soumissions en phases (PCSP) décrit ci-dessous pour ce besoin SEULEMENT si le Canada reçoit 4 soumissions ou moins avant la date de clôture de la demande de soumissions.

b) Nonobstant tout examen par le Canada aux phases I ou II du Processus, les soumissionnaires sont et demeureront les seuls et uniques responsables de l'exactitude, de l'uniformité et de l'exhaustivité de leurs soumissions, et le Canada n'assume, en vertu de cet examen, aucune obligation ni de responsabilité envers les soumissionnaires de relever, en tout ou en partie, toute erreur ou toute omission, dans les soumissions ou en réponse à toute communication provenant d'un soumissionnaire.

LE SOUMISSIONNAIRE RECONNAÎT QUE LES EXAMENS LORS DES PHASES I ET II DU PRÉSENT PROCESSUS NE SONT QUE PRÉLIMINAIRES ET N'EMPÊCHENT PAS QU'UNE SOUMISSION SOIT NÉANMOINS JUGÉE NON RECEVABLE À LA PHASE III, ET CE, MÊME POUR LES EXIGENCES OBLIGATOIRES QUI ONT FAIT L'OBJET D'UN EXAMEN AUX PHASES I OU II, ET MÊME SI LA SOUMISSION AURAIT ÉTÉ JUGÉE RECEVABLE À UNE PHASE ANTÉRIEURE. LE CANADA PEUT DÉTERMINER À SA DISCRÉTION QU'UNE SOUMISSION NE RÉPOND PAS À UNE EXIGENCE OBLIGATOIRE À N'IMPORTE QUELLE DE CES PHASES. LE SOUMISSIONNAIRE RECONNAÎT ÉGALEMENT QUE MALGRÉ LE FAIT QU'IL AIT FOURNI UNE RÉPONSE À UN AVIS OU À UN RAPPORT D'ÉVALUATION DE LA CONFORMITÉ (REC) (TEL QUE CES TERMES SONT DÉFINIS PLUS BAS) QU'IL EST POSSIBLE QUE CETTE RÉPONSE NE SUFFISE PAS POUR QUE SA SOUMISSION SOIT JUGÉE CONFORME AUX AUTRES EXIGENCES OBLIGATOIRES.

c) Le Canada peut, à sa propre discrétion et à tout moment, demander et recevoir de l'information de la part du soumissionnaire afin de corriger des erreurs ou des lacunes administratives dans sa soumission, et cette nouvelle information fera partie intégrante de sa soumission. Ces erreurs pourraient être, entre autres : une signature absente; une case non cochée dans un formulaire; une erreur de forme; l'omission d'un accusé de réception, du numéro d'entreprise d'approvisionnement ou même les coordonnées des personnes-ressources, c'est-à-dire leurs noms, leurs adresses et les numéros de téléphone; ou encore des erreurs d'inattention dans les calculs ou dans les nombres, et des erreurs qui n'affectent en rien les montants que le soumissionnaire a indiqué pour le prix ou pour tout composant du prix. Ainsi, le Canada a le droit de demander ou de recevoir toute information après la date de clôture de l'invitation à soumissionner uniquement lorsque l'invitation à soumissionner permet ce droit expressément. Le soumissionnaire disposera alors d'un délai indiqué pour fournir l'information requise. Toute information fournie hors délais sera refusée.

d) Le PCSP ne limite pas les droits du Canada en vertu du Guide des CCUA 2003 Instructions uniformisées – biens ou services – besoins concurrentiels, ni le droit du Canada de demander ou d'accepter toute information pendant la période de soumission ou après la clôture de cette dernière, lorsque la demande de soumissions confère expressément ce droit au Canada, ou dans les circonstances décrites au paragraphe (c).

e) Le Canada enverra un Avis ou un REC selon la méthode de son choix et à sa discrétion absolue. Le soumissionnaire doit soumettre sa réponse par la méthode stipulée dans l'Avis ou le REC. Les réponses sont réputées avoir été reçues par le Canada à la date et à l'heure qu'elles ont été livrées au Canada par la méthode indiquée dans l'Avis ou le REC et à l'adresse qui y figure. Un courriel de réponse autorisé dans l'Avis ou le REC est réputé reçu par le Canada à la date et à l'heure auxquelles il a été reçu dans la boîte de réception de l'adresse électronique indiquée dans l'Avis ou le REC. Un Avis, ou un REC, envoyé par le Canada au soumissionnaire à l'adresse fournie par celui-ci dans la soumission ou après l'envoi de celle-ci est réputé avoir été reçu par le soumissionnaire à la date à laquelle il a été envoyé par le Canada. Le Canada n'assume aucune responsabilité envers les soumissionnaires pours les soumissions retardataires, peu importe la cause.

4.1.1.2 Phase I : soumission financière

a) Après la date et l'heure de clôture de cette demande de soumissions, le Canada examinera la soumission pour déterminer si elle comporte une soumission financière et si celle-ci contient toute l'information demandée par la demande de soumissions. L'examen par le Canada à la phase I se limitera à déterminer s'il y manque des informations exigées par la demande de soumissions à la soumission financière. Cet examen n'évaluera pas si la soumission financière répond à toute norme ou si elle est conforme à toutes les exigences de la demande.

b) L'examen par le Canada durant la phase I sera effectué par des fonctionnaires du ministère des TPSGC.

c) Si le Canada détermine, selon sa discrétion absolue, qu'il n'y a pas de soumission financière ou qu'il manque toutes les informations demandées dans la soumission financière, la soumission sera alors jugée non recevable et sera rejetée.

d) Pour les soumissions autres que celles décrites au paragraphe (c), Canada enverra un avis écrit au soumissionnaire (« Avis ») identifiant où la soumission financière manque d'informations. Un soumissionnaire dont la soumission financière a été jugée recevable selon les exigences examinées lors de la phase I ne recevra pas d'Avis. De tels soumissionnaires n'auront pas le droit de soumettre de l'information supplémentaire relativement à leur soumission financière.

e) Les soumissionnaires qui ont reçu un Avis bénéficieront d'un délai indiqué dans l'Avis (la « période de grâce ») pour redresser les points indiqués dans l'Avis en fournissant au Canada, par écrit, l'information supplémentaire ou une clarification en réponse à l'Avis. Les réponses reçues après la fin de la période de grâce ne seront pas prises en considération par le Canada sauf dans les circonstances et conditions stipulées expressément dans l'avis.

f) Dans sa réponse à l'Avis, le soumissionnaire n'aura le droit de redresser que la partie de sa soumission financière indiquée dans l'Avis. Par exemple, lorsque l'Avis indique qu'un élément a été laissé en blanc, seule l'information manquante pourra ainsi être ajoutée à la soumission financière, excepté dans les cas où l'ajout de cette information entraînera nécessairement la modification des calculs qui ont déjà été présentés dans la soumission financière (p. ex. le calcul visant à déterminer le prix total). Les rajustements nécessaires devront alors être mis en évidence par le soumissionnaire et seuls ces rajustements pourront être effectués. Toutes les informations fournies doivent satisfaire aux exigences de la demande de soumissions.

g) Toute autre modification apportée à la soumission financière soumise par le soumissionnaire sera considérée comme une nouvelle information et sera rejetée. Aucun changement ne sera autorisé à une quelconque autre section de la soumission du soumissionnaire. L'intégralité de l'information soumise conformément aux exigences de cette demande de soumissions en réponse à l'Avis remplacera uniquement la partie de la soumission financière originale telle qu'autorisée ci-dessus et sera utilisée pour le reste du processus d'évaluation des soumissions.

h) Le Canada déterminera si la soumission financière est recevable pour les exigences examinées à la phase I, en tenant compte de l'information supplémentaire ou de la clarification fournie par le soumissionnaire conformément à la présente section. Si la soumission financière n'est pas jugée recevable au regard des exigences examinées à la phase I à la satisfaction du Canada, la soumission financière sera jugée non recevable et rejetée.

i) Seules les soumissions jugées recevables conformément aux exigences examinées à la phase I à la satisfaction du Canada seront examinées à la phase II.

4.1.1.3 Phase II : soumission technique

a) L'examen par le Canada au cours de la phase II se limitera à une évaluation de la soumission technique afin de vérifier si le soumissionnaire a respecté toutes les exigences obligatoires d'admissibilité. Cet examen n'évalue pas si la soumission technique répond à une norme ou répond à toutes les exigences de la soumission. Les exigences obligatoires d'admissibilité sont les critères techniques obligatoires tels qu'ainsi décrits dans la présente demande de soumissions comme faisant partie du Processus de conformité des soumissions en phases. Les critères techniques obligatoires qui ne sont pas identifiés dans la demande de soumissions comme faisant partie du PCSP ne seront pas évalués avant la phase III.

b) Le Canada enverra un avis écrit au soumissionnaire REC précisant les exigences obligatoires d'admissibilité que la soumission n'a pas respectée. Un soumissionnaire dont la soumission a été jugée recevable au regard des exigences examinées au cours de la phase II recevra un REC qui précisera que sa soumission a été jugée recevable au regard des exigences examinées au cours de la phase II. Le soumissionnaire en question ne sera pas autorisé à soumettre des informations supplémentaires en réponse au REC.

c) Le soumissionnaire disposera de la période de temps précisée dans le REC (« période de grâce ») pour remédier à l'omission de répondre à l'une ou l'autre des exigences obligatoires d'admissibilité inscrites dans le REC en fournissant au Canada, par écrit, des informations supplémentaires ou des clarifications en réponse au REC. Les réponses reçues après la fin de la période de grâce ne seront pas prises en considération par le canada sauf, dans les circonstances et conditions expressément prévues par le REC.

d) La réponse du soumissionnaire doit adresser uniquement les exigences obligatoires d'admissibilité énumérées dans le rapport d'évaluation de conformité (REC) et considérées comme non accomplies, et doit inclure uniquement les renseignements nécessaires pour ainsi se conformer aux exigences. Toutefois, dans le cas où une réponse aux exigences obligatoires d'admissibilité énumérées dans le REC entraînera nécessairement la modification d'autres renseignements qui sont déjà présents dans la soumission, les rajustements nécessaires devront être mis en évidence par le soumissionnaire. La réponse au REC ne doit pas inclure de changement à la soumission financière. Toute autre information supplémentaire qui n'est pas requise pour se conformer aux exigences ne sera pas prise en considération par le Canada.

e) La réponse du soumissionnaire au REC devra spécifier, pour chaque cas, l'exigence obligatoire d'admissibilité du REC à laquelle elle répond, notamment en identifiant le changement effectué dans la section correspondante de la soumission initiale, et en identifiant dans la soumission initiale les modifications nécessaires qui en découlent. Pour chaque modification découlant de la réponse aux exigences obligatoires d'admissibilité énumérées dans le REC, le soumissionnaire doit expliquer pourquoi une telle modification est nécessaire. Il n'incombe pas au Canada de réviser la soumission du soumissionnaire; il incombe plutôt au soumissionnaire d'assumer les conséquences si sa réponse au REC n'est pas effectuée conformément au présent paragraphe. Toutes les informations fournies doivent satisfaire aux exigences de la demande de soumissions.

f) Tout changement apporté à la soumission par le soumissionnaire en dehors de ce qui est demandé, sera considéré comme étant de l'information nouvelle et ne sera pas prise en considération. L'information soumise selon les exigences de cette demande de soumissions en réponse au REC remplacera, intégralement et uniquement la partie de la soumission originale telle qu'elle est autorisée dans cette section.

g) Les informations supplémentaires soumises pendant la phase II et permises par la présente section seront considérées comme faisant partie de la soumission et seront prises en compte par le Canada dans l'évaluation de la soumission lors de la phase II que pour déterminer si la soumission respecte les exigences obligatoires admissibles. Celles-ci ne seront utilisées à aucune autre phase de l'évaluation pour augmenter ou diminuer les notes que la soumission originale pourrait obtenir sans les avantages de telles informations additionnelles. Par exemple, un critère obligatoire admissible qui exige l'obtention d'un nombre minimum de points pour être considéré conforme sera évalué à la phase II afin de déterminer si cette note minimum obligatoire aurait été obtenue si le soumissionnaire avait soumis les renseignements supplémentaires en réponse au REC. Dans ce cas, la soumission sera considérée comme étant conforme par rapport à ce critère obligatoire admissible et les renseignements supplémentaires soumis par le soumissionnaire lieront le soumissionnaire dans le cadre de sa soumission, mais la note originale du soumissionnaire, qui était inférieure à la note minimum obligatoire pour ce critère obligatoire admissible, ne changera pas, et c'est cette note originale qui sera utilisée pour calculer les notes pour la soumission.

h) Le Canada déterminera si la soumission est recevable pour les exigences examinées à la phase II, en tenant compte de l'information supplémentaire ou de la clarification fournie par le soumissionnaire conformément à la présente section. Si la soumission n'est pas jugée recevable selon des exigences examinées à la phase II à la satisfaction du Canada, la soumission sera jugée non recevable et rejetée.

i) Uniquement les soumissions jugées recevables selon les exigences examinées à la phase II et à la satisfaction du Canada seront ensuite évaluées à la phase III.

4.1.1.4 Phase III : évaluation finale de la soumission

a) À la phase III, le Canada complétera l'évaluation de toutes les soumissions jugées recevables selon les exigences examinées à la phase II. Les soumissions seront évaluées par rapport à l'ensemble des exigences de la demande de soumissions, y compris les exigences d'évaluation technique et financière.

b) Une soumission sera jugée non recevable et sera rejetée si elle ne respecte pas toutes les exigences d'évaluation obligatoires de la demande de soumissions.

4.1.2 Évaluation technique

4.1.2.1 Expérience de la coentreprise

a) Lorsque le soumissionnaire est une coentreprise qui possède de l'expérience à ce titre, il peut soumettre l'expérience qu'il a acquise dans le cadre de cette coentreprise.

Exemple : Un soumissionnaire est une coentreprise formée des membres L et O. La demande de soumissions exige que le soumissionnaire possède de l'expérience en prestation de services de maintenance et dépannage à un client comptant au moins 10 000 utilisateurs pendant 24 mois. En tant que coentreprise (composée de L et O), le soumissionnaire a déjà réalisé ce travail. Il peut donc utiliser cette expérience pour satisfaire à l'exigence. Si L a acquis cette expérience alors qu'il était en coentreprise avec une tierce partie, N, cette expérience ne peut pas être utilisée parce que N ne fait pas partie de la coentreprise qui présente une soumission.

b) Une coentreprise qui présente une soumission peut évoquer l'expérience de l'un de ses membres pour démontrer qu'elle satisfait à tout critère technique de la présente demande de soumissions.

Exemple : Un soumissionnaire est membre d'une coentreprise composée de X, Y et Z. Si une demande de soumissions exige : (a) que le soumissionnaire ait trois ans d'expérience de la prestation de services de maintenance, et (b) que le soumissionnaire ait deux ans d'expérience de l'intégration de matériel à des réseaux complexes, chacune de ces deux exigences peut être satisfaite par un membre différent de la coentreprise. Cependant, pour un critère donné, par exemple celui qui concerne l'expérience de trois ans de la prestation de services de maintenance, le soumissionnaire ne peut pas indiquer que chaque membre, soit X, Y et Z, a un an d'expérience pour un total de trois ans. Une telle réponse serait déclarée non conforme.

c) Les membres de la coentreprise ne peuvent cependant pas mettre ensemble leurs capacités pour répondre à un critère technique donné de la présente demande de soumissions. Un membre de la coentreprise peut néanmoins mettre sa propre expérience en commun avec celle de la coentreprise. Chaque fois qu'il doit faire la preuve qu'il répond à un critère, le soumissionnaire doit indiquer quel membre de la coentreprise y répond. Si le soumissionnaire n'a pas indiqué quel membre de la coentreprise répond à l'exigence, l'autorité contractante lui donnera l'occasion de fournir ce renseignement pendant la période d'évaluation. Si le soumissionnaire ne fournit pas ce renseignement pendant la période fixée par l'autorité contractante, sa soumission sera déclarée non recevable.

Exemple : Un soumissionnaire est membre d'une coentreprise composée de A et B. Si, dans une demande de soumissions, on exige que le soumissionnaire ait de l'expérience dans la prestation de ressources pour un minimum de 100 jours facturables, le soumissionnaire peut démontrer son expérience en présentant ce qui suit :

- les contrats signés par A;
- les contrats signés par B; ou
- les contrats signés par A et B en coentreprise; ou
- les contrats signés par A et les contrats signés par A et B en coentreprise; ou
- les contrats signés par B et les contrats signés par A et B en coentreprise.

Le tout doit totaliser 100 jours facturables.

d) Tout soumissionnaire ayant des questions sur la façon dont la soumission d'une coentreprise sera évaluée devrait poser ces questions dans le cadre du processus de demande de renseignements dès que possible pendant la période de soumission.

4.1.2.2 Critères techniques obligatoires

Voir la pièce jointe 1 de la Partie 4. Le PCSP s'appliquera uniquement aux exigences techniques obligatoires indiquées par l'exposant (^{SP}). Les exigences techniques obligatoires non affectées de l'exposant (^{SP}) ne seront pas assujettis au PCSP.

4.1.2.3 Visite d'évaluation des installations

Le Canada pourrait visiter l'installation proposée dans la soumission évaluée la plus basse et recevable au plan technique afin de confirmer qu'elle est telle que décrite dans la soumission et qu'elle satisfait aux exigences techniques décrites dans la demande de soumissions.

L'authorité'autorité contractante allouera au soumissionnaire un préavis d'au moins 10 jours ouvrables avant la visite de l'installation pour effectuer la validation. Le Canada visitera ensuite l'installation et effectuera la validation. La visite de validation sera achevée dans un délai de deux jours ouvrables. Le Canada assumera les frais associés à la validation de la visite des lieux.

Le soumissionnaire accorde au Canada, aux fins de la validation, le droit d'accéder à l'installation et à tous les lieux inclus dans la soumission.

Le Canada documentera les résultats de la validation de la visite de l'installation. Si le Canada détermine que le soumissionnaire ne répond pas aux exigences indiquées dans la Pièce jointe 1 de la Partie 4 de la demande de soumissions, le soumissionnaire échouera à la validation et la soumission sera déclarée non-recevable. Le soumissionnaire aura la possibilité de répondre et de fournir une preuve de la façon dont il répond aux critères indiqués comme non-recevable.

4.1.3 Évaluation financière

Aux fins de l'évaluation des soumissions et de la sélection de l'entrepreneur, le prix évalué d'une soumission sera déterminé conformément au barème de prix détaillé dans la pièce jointe 1 de la Partie 3.

4.2 Méthode de selection - prix évalué le plus bas

a) Une soumission doit respecter les exigences de la demande de soumissions et satisfaire à tous les critères d'évaluation obligatoires pour être déclarée recevable; et

b) La soumission recevable ayant le prix évalué le plus bas sera recommandée pour attribution d'un contrat.

PIÈCE JOINTE 1 DE LA PARTIE 4, CRITÈRES TECHNIQUES

Critères techniques obligatoires

Les soumissions doivent satisfaire à tous les critères techniques obligatoires indiqués ci-dessous. Le soumissionnaire doit fournir la documentation nécessaire afin de démontrer qu'il se conforme à cette exigence.

Les soumissions qui ne satisfont pas à tous les critères techniques obligatoires seront déclarées irrecevables. Chaque critère technique obligatoire devrait être traité séparément.

Critères techniques obligatoires

Pour l'évaluation des critères techniques obligatoires mentionnés ci-dessous, l'expérience du soumissionnaire, de ses sous-traitants, de ses sociétés affiliées et de ses fournisseurs sera prise en considération.

Nombre	Critère technique obligatoire (TO)	Instructions à l'intention des soumissionnaires
TO1	Le soumissionnaire doit avoir été en activité pendant au moins trois ans avant la date de publication de la demande de soumissions.	Le soumissionnaire doit fournir ce qui suit : Une copie du certificat d'enregistrement du nom commercial; OU Une copie du certificat d'enregistrement de la société par actions provincial ou territorial; OU Une copie du certificat fédéral d'enregistrement de l'incorporation de l'entreprise. OU Référence à la loi incorporant l'établissement d'enseignement.

Critères techniques obligatoires

Pour l'évaluation des critères techniques obligatoires mentionnés ci-dessous, l'expérience du soumissionnaire, de ses sous-traitants, de ses sociétés affiliées et de ses fournisseurs sera prise en considération.

Nombre	Critère technique obligatoire (TO)	Instructions à l'intention des soumissionnaires
TO2[SP]	Le programme de formation des cyberopérateurs du soumissionnaire doit être reconnu par une autorité scolaire canadienne reconnue par la province. Un organisme de formation, comme un collège ou une université, est acceptable et peut comprendre divers cours. Cependant, il doit être reconnu par une autorité scolaire canadienne reconnue par la province selon l'exigence TO2.	Le soumissionnaire doit fournir : a) Documents juridiques (par exemple, certificat d'accréditation, charte), sauf s'il s'agit d'une université constituée en vertu de la loi; b) Politiques d'évaluation des stagiaires, procédures de notation et grilles de notation; c) Politiques et procédures d'assistance par tuteurs (une ébauche est acceptable); d) Toutes les directives, les règles et les réglementations fournies aux stagiaires, y compris la politique de changement de cours; et e) Une copie vierge et non signée du diplôme ou certificat qui serait fourni à un stagiaire ayant réussi ce programme.

Critères techniques obligatoires

Pour l'évaluation des critères techniques obligatoires mentionnés ci-dessous, l'expérience du soumissionnaire, de ses sous-traitants, de ses sociétés affiliées et de ses fournisseurs sera prise en considération.

Nombre	Critère technique obligatoire (TO)	Instructions à l'intention des soumissionnaires
TO3[SP]	L'outil d'évaluation du soumissionnaire doit permettre d'évaluer les compétences des cyberopérateurs par rapport au matériel de formation cybernétique de qualification de niveau soldat (sdt) (QG) (DP1) du contrat W4938-20069S/001/ZH, voir les appendices 1 à 3 de l'annexe A, Énoncé des travaux.	Le soumissionnaire doit fournir une description détaillée de la façon dont son outil d'évaluation : a) Sera livré dans les 30 jours civils suivant l'attribution du contrat; et b) Permettra d'évaluer les compétences du cyberopérateur par rapport au cours de QG sdt (PP1); cette description détaillée doit comprendre : i. Comment leur outil d'évaluation en cours sera utilisé et/ou sur mesure pour répondre aux objectifs de performance de l'opérateur cyber (OREN 001 – OREN 005) à l'appendice 2 de l'annexe A; ii. La capacité d'effectuer des évaluations à distance en fonction du rythme opérationnel du personnel du Centre d'opérations du réseau des Forces canadiennes (CORFC); et iii. Une analyse clairement définie de la partie du cours de QG sdt (PP1) qui doit faire l'objet d'un perfectionnement professionnel plus poussé. Une analyse clairement définie consiste à montrer quel matériel de cyberformation du QG sdt le cyberopérateur doit approfondir.

Critères techniques obligatoires

Pour l'évaluation des critères techniques obligatoires mentionnés ci-dessous, l'expérience du soumissionnaire, de ses sous-traitants, de ses sociétés affiliées et de ses fournisseurs sera prise en considération.

Nombre	Critère technique obligatoire (TO)	Instructions à l'intention des soumissionnaires
TO4[SP]	La trousse de formation de perfectionnement professionnel (PP) de cyberopérateur des soumissionnaires doit pouvoir répondre aux exigences visant le matériel de cours de QG sdt (PP1) du contrat W4938-20069S/001/ZH, voir les appendices 1 à 3 de l'annexe A, Énoncé des travaux.	Le soumissionnaire doit fournir une description détaillée de la façon dont la trousse de formation de PP : a) Répond aux exigences de l'outil d'évaluation; b) Répond aux exigences de la QG sdt (PP1); c) Sera évaluée et approuvée par le bureau du programme d'accréditations, de certifications et d'équivalences des Forces armées canadiennes avant la livraison de la trousse de formation de perfectionnement professionnel aux stagiaires; d) Durera au maximum 3 mois; et e) Sera livrée dans les 30 jours civils après avoir livré les résultats de l'outil d'évaluation.
TO5[SP]	Le site et les installations de formation du soumissionnaire doivent être capables d'offrir un apprentissage virtuel à distance, afin de répondre à toutes les exigences de la trousse de formation de perfectionnement professionnel.	Le soumissionnaire doit fournir une description détaillée et démontrer comment il répond aux exigences en matière d'apprentissage virtuel, ce qui comprend : a) Fournir aux stagiaires l'équipement informatique approprié pour effectuer un apprentissage à distance; b) Offrir un horaire d'apprentissage en ligne souple pour répondre aux exigences opérationnelles et aux besoins du personnel du CORFC, ce qui peut nécessiter un apprentissage à distance en dehors du bureau; c) La capacité d'offrir des leçons dirigées avec instructeur à distance; d) La capacité d'offrir des leçons dans un cyberlaboratoire à distance; e) La capacité de tenir des exercices d'entraînement collectif virtuels à distance; et f) La possibilité d'évaluer les stagiaires à distance.
TO6	Le soumissionnaire doit posséder un site et des installations de formation à Kingston, en Ontario ou dans la région de la capitale nationale.	Le soumissionnaire doit fournir l'adresse complète du site et des installations de formation (adresse municipale, municipalité/ville, province et code postal).

Critères techniques obligatoires Pour l'évaluation des critères techniques obligatoires mentionnés ci-dessous, l'expérience du soumissionnaire, de ses sous-traitants, de ses sociétés affiliées et de ses fournisseurs sera prise en considération.		
Nombre	Critère technique obligatoire (TO)	Instructions à l'intention des soumissionnaires
TO7[SP]	Le site et les installations de formation du soumissionnaire doivent comporter une salle de classe ou un laboratoire informatique répondant aux exigences suivantes : a) Doit accueillir jusqu'à 24 stagiaires; b) Doit être équipé de bureaux et de chaises pour accueillir jusqu'à 24 stagiaires; c) Doit être équipé d'au moins 24 ordinateurs ou ordinateurs portables; d) Doit être muni des périphériques nécessaires aux cyberopérations et de la capacité de configurer son réseau de support d'information; e) Doi être muni d'un serveur et d'une infrastructure de réseau permettant d'atteindre les objectifs de formation pour le traitement et le stockage des informations à distribution limitée; et f) Doit être muni d'un photocopieur.	Le soumissionnaire doit fournir une description détaillée de la salle de classe ou du laboratoire informatique afin de démontrer qu'il répond aux exigences énoncées.
TO8[SP]	Le site et les installations de formation du soumissionnaire doivent comporter une salle à manger répondant aux exigences suivantes : a) Doit être séparée de la salle de classe ou du laboratoire informatique; b) Doit accueillir jusqu'à 24 stagiaires afin que ces derniers puissent prendre leur repas en groupe; c) Doit être équipée d'un réfrigérateur; et d) Doit être équipée d'un four micro-ondes.	Le soumissionnaire doit fournir une description détaillée de la salle à manger afin de démontrer qu'elle répond aux exigences énoncées.

Critères techniques obligatoires

Pour l'évaluation des critères techniques obligatoires mentionnés ci-dessous, l'expérience du soumissionnaire, de ses sous-traitants, de ses sociétés affiliées et de ses fournisseurs sera prise en considération.

Nombre	Critère technique obligatoire (TO)	Instructions à l'intention des soumissionnaires
TO9[SP]	Le soumissionnaire doit présenter un plan de ressources humaines qui permet de recruter et de remplacer des ressources qualifiées afin de fournir les services énoncés à l'annexe A, Énoncé des travaux.	Le soumissionnaire doit fournir les éléments suivants ou le lien menant à la page Web appropriée : a) Le processus de présélection et de sélection des professeurs, instructeurs et aides-enseignants qualifiés de la faculté; b) La stratégie et le processus permettant de respecter le ratio stagiaire et professeur/instructeur/aide-enseignant de 12:1; c) La stratégie et le processus utilisés pour remplacer les ressources qualifiées dans les délais afin d'éviter l'interruption des services.

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 fausse, 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.

Les soumissionnaires doivent compléter leurs attestations exigées à la Partie 5 en utilisant le formulaire PDF à la pièce jointe 2 de la Partie 3.

PARTIE 6 - EXIGENCES RELATIVES À LA SÉCURITÉ

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'organisme valable, tel qu'indiqué à la Partie 7 - Clauses du contrat subséquent; et

b) Si l'information n'est pas fournie dans ou avec la soumission, l'autorité contractante en informera le soumissionnaire et lui donnera un délai afin de se conformer aux exigences. Le défaut de répondre à la demande de l'autorité contractante et de se conformer aux exigences dans les délais prévus aura pour conséquence le rejet de la soumission.

6.1.2 On rappelle aux soumissionnaires d'obtenir rapidement la cote de sécurité requise. La décision de retarder l'attribution du contrat, pour permettre au soumissionnaire retenu d'obtenir la cote de sécurité requise, demeure à l'entière discrétion de l'autorité contractante.

6.1.3 Pour de plus amples renseignements sur les exigences relatives à la sécurité, les soumissionnaires devraient consulter le site Web du Programme de sécurité des contrats de TPSGC (http://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, à l'Annexe A.

7.2 Clauses et conditions uniformisées

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

7.2.1 Conditions générales

2035 (2020-05-28), Conditions générales - besoins plus complexes de services, s'appliquent au contrat et en font partie intégrante.

7.2.2 Conditions générales supplémentaires

4007 (2010-08-16), Le Canada détient les droits de propriété intellectuelle sur les renseignements originaux, s'appliquent au contrat et en font partie intégrante.

7.2.3 Entente de non-divulgation

L'entrepreneur doit obtenir de son ou ses employé(s) ou sous-traitant(s) l'entente de non-divulgation, inclue à l'annexe C, remplie et signée et l'envoyer au responsable à le Responsable technique avant de leur donner accès aux renseignements fournis par ou pour le Canada relativement aux travaux.

7.3 Exigences relatives à la sécurité

a) Les exigences relatives à la sécurité suivantes (la liste de vérification des exigences relatives à la sécurité (LVERS) et clauses connexes), tel que prévu par le Programme de sécurité des contrats (PSC) (https://www.tpsgc-pwgsc.gc.ca/esc-src/introduction-fra.html), s'appliquent et font partie intégrante du contrat :

1. L'entrepreneur doit détenir en permanence, pendant l'exécution du contrat, une attestation de vérification d'organisation désignée (VOD) en vigueur, délivrée par le PSC, TPSGC;
2. Les membres du personnel de l'entrepreneur devant avoir accès à des renseignements ou à des biens PROTÉGÉS, ou à des établissements dont l'accès est réglementé, doivent TOUS détenir une cote de FIABILITÉ en vigueur, délivrée ou approuvée par le PSC, TPSGC;
3. L'entrepreneur NE DOIT PAS emporter de renseignements ou de biens PROTÉGÉS hors des établissements visés; et l'entrepreneur doit s'assurer que son personnel est au courant de cette restriction et qu'il la respecte;
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; et
5. L'entrepreneur ou l'offrant doit respecter les dispositions :

    i. De la LVERS, reproduite ci-joint à l'Annexe B; et
    ii. Du *Manuel de la sécurité industrielle* (dernière édition).

b) L'agent de sécurité d'entreprise (ASE) doit s'assurer, par l'entremise du PSC, que le soumissionnaire et les individus proposés sont titulaires d'une cote de sécurité en vigueur et au niveau exigé.

7.4 Utilisation des équipements de protection individuelle et lignes directrices en matière de santé et de sécurité au travail

a) Le fournisseur doit se conformer aux exigences du Gouvernement du Canada en lien avec le port d'équipement(s) de protection individuelle dans les bureaux du Gouvernement du Canada et suivre à tout moment les directives en matière de santé et de sécurité au travail (SST) en vigueur sur ces lieux de travail.

b) Le fournisseur procurera à ses ressources l'équipement de protection individuelle suivant pour ces lieux de travail: [modifier la liste d'équipement(s) de protection individuelle qui suit tel que requis] masques prescrits couvrant le visage, gants, visière de protection, et tout autre équipement requis pour entrer ou travailler sur les lieux de travail du Gouvernement du Canada. Le Canada se réserve le droit de modifier la ligne directrice en matière de SST ou la liste d'équipement de protection individuelle, au besoin, pour y inclure toute recommandation future proposée par les organismes de santé publique.

c) L'entrepreneur garantit que ses ressources suivront à tout moment les directives SST en vigueur sur ces lieux de travail pendant la durée du contrat que celles-ci porteront tout équipement de protection individuelle mentionné ci-haut sur ces lieux de travail. Toute ressource qui ne porte pas l'équipement de protection individuelle requis et/ou qui ne suit pas les directives SST en vigueur sur les lieux de travail se verra refuser l'accès aux lieux de travail du Gouvernement du Canada.

7.5 Durée du contrat

7.5.1 Période du contrat

La période du contrat est à partir de la date du contrat jusqu'au 31 décembre 2022 inclusivement.

7.5.2 Résiliation avec avis de 120 jours

Le Canada se réserve le droit de résilier à n'importe quel moment le contrat, en tout ou en partie, en donnant un avis écrit de 120 jours civils à l´entrepreneur.

Suite à cette résiliation, le Canada paiera uniquement les coûts engagés pour les services rendus et acceptés par le Canada avant la date de la résiliation. Malgré toute autre disposition du contrat, aucun autre coût résultant de la résiliation ne sera payé à l´entrepreneur.

7.5.3 Ententes sur les revendications territoriales globales

Le contrat ne comprend pas de demandes de livraison de services à faire dans les zones visées par des ententes sur les revendications territoriales globales (ERTG) au sein du Yukon, des Territoires du Nord-Ouest, du Nunavut, du Québec ou du Labrador. Toute demande de livraison de services à faire dans les zones visées par des ERTG au sein du Yukon, des Territoires du Nord-Ouest, du Nunavut, du Québec ou du Labrador devra faire partie d'un contrat distinct.

7.6 Responsables

7.6.1 Autorité contractante

L'autorité contractante pour le contrat est :

Diane Reynolds
Spécialiste en approvisionnement
Direction générale des approvisionnements
Direction de l'acquisition des services professionnels
Les Terrasses de la Chaudière
10, rue Wellington, 5ième étage
Gatineau (Québec), K1A OS5
Téléphone : 873-469-3941
Télécopieur : 819-956-9235
Courriel : Diane.Reynolds@tpsgc-pwgsc.gc.ca

L'autorité contractante est responsable de la gestion du contrat, et toute modification doit être autorisée par écrit par l'autorité contractante. L'entrepreneur ne doit pas effectuer de travaux dépassant la portée du contrat ou des travaux qui n'y sont pas prévus, suite à des demandes ou instructions verbales ou écrites de toute personne autre que l'autorité contractante.

7.6.2 Responsable technique

Le responsable technique pour le contrat est :

À insérer au moment de l'attribution du contrat

Le responsable technique 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 responsable technique; 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 de contrat émise par l'autorité contractante.

7.6.3 Représentant de l'entrepreneur

À insérer au moment de l'attribution du contrat

7.7 Paiement

7.7.1 Base de paiement

7.7.1.1 Taux fixe journalier

a) Pour le developer/livrer du outil d'évaluation et la trousse de formation de perfectionnement professionnel à le client, l'entrepreneur sera payé un taux fixe journalier tout compris figurant ci-dessous. Le taux fixe journalier tout compris comprend tous les coûts associés avec developer/livrer du outil d'évaluation et la trousse de formation de perfectionnement professionnel à le client; les droits de douane sont inclus et les taxes applicables sont en sus.

Taux fixe journalier tout compris : *À insérer au moment de l'attribution du contrat* $

b) Aux fins du contrat, la journée de travail comprend 7,5 heures, à l'exclusion des pauses-repas. On paiera les jours de travail réels, sans provision pour les vacances annuelles, les jours fériés et les congés de maladie. Si la durée du temps de travail est supérieure ou inférieure à la journée de travail, le taux fixe journalier tout compris sera rajusté proportionnellement pour tenir compte du nombre réel d'heures de travail.

7.7.1.2 Prix unitaire ferme

a) Pour l'évaluation des stagiaires utilisant l'outil d'évaluation, l'entrepreneur sera payé un prix unitaire ferme par participant figurant ci-dessous. Le prix unitaire ferme par participant comprend tous les coûts associés à l'évaluation des stagiaires utilisant l' outil d'évaluation, les droits de douane sont inclus et les taxes applicables sont en sus.

Prix unitaire ferme par stagiaire : *À insérer au moment de l'attribution du contrat* $

b) Pour le livrer de la formation de perfectionnement professionnel aux stagaires, l'entrepreneur sera payé un prix unitaire ferme par stagiaire figurant ci-dessous jusqu'à un maximum de 24 stagiaires par classe. Le prix unitaire ferme par stagiaire comprend tous les coûts associés à la prestation de formation aux stagiaires (p. ex. matériel en technologie de l'information, le logiciel, le courriel individuel pour le stagiaire, etc.), les droits de douane sont inclus et les taxes applicables sont en sus.

Prix unitaire ferme par stagiaire : *À insérer au moment de l'attribution du contrat* $

c) Le Canada ne paiera pas l'entrepreneur pour tout changement à la conception, toute modification ou interprétation des travaux, à moins que ces changements à la conception, ces modifications ou ces interprétations n'aient été approuvés par écrit par l'autorité contractante avant d'être intégrés aux travaux.

7.7.1.3 Frais administratifs

En ce qui concerne les manuels neufs ou de rechange, le soumissionnaire sera remboursé au prix coûtant, plus les frais administratifs. Ces derniers comprennent l'ensemble des coûts associés à la fourniture du manuel au client. Les droits de douane sont inclus et les taxes applicables sont en sus.

Frais administratifs : *À insérer au moment de l'attribution du contrat* %

7.7.2 Responsabilité totale du Canada

a) La responsabilité totale du Canada envers l'entrepreneur en vertu du contrat ne doit pas dépasser la somme de *À insérer au moment de l'attribution du contrat* $. Les droits de douane sont inclus et les taxes applicables sont en sus;

b) 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 une augmentation de la responsabilité totale du Canada à moins que l'augmentation n'ait été autorisée par écrit par l'autorité contractante. L'entrepreneur doit informer, par écrit, l'autorité contractante :

i. lorsque 75 p. 100 de la somme est engagée, ou
ii. quatre mois avant la date d'expiration du contrat, ou
iii. 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;

c) 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 requis. La présentation de cette information par l'entrepreneur n'augmente pas automatiquement la responsabilité du Canada à son égard.

7.7.3 Méthode de paiement

7.7.3.1 Paiement mensuel

a) Pour le développer/livrer du outil d'évaluation, l'évaluation des stagiaires utilisant l'outil d'évaluation, et le developer/livrer de la trousse de formation de perfectionnement professionnel à le client, le Canada paiera l'entrepreneur chaque mois pour les travaux complétés pendant le mois visé par la facture conformément aux dispositions de paiement du contrat si :

i. 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;
ii. tous ces documents ont été vérifiés par le Canada; et
iii. les travaux livrés ont été acceptés par le Canada.

7.7.3.2 Paiement unique

a) Pour le livrer de la formation de perfectionnement professionnel aux stagaires ou en ce qui concerne les manuels neufs ou de rechange, le Canada paiera l'entrepreneur lorsque les travaux seront terminés et livrés conformément aux dispositions de paiement du contrat si :

i. 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;
ii. tous ces documents ont été vérifiés par le Canada; et
iii. les travaux livrés ont été acceptés par le Canada.

7.7.4 Clauses du guide des CCUA

A9117C (2007-11-30), T1204 - demande directe du ministère client

7.7.5 Paiement électronique de factures – contrat (s'il y a lieu)

L'entrepreneur accepte d'être payé au moyen de l'un des instruments de paiement électronique suivants :

a) Carte d'achat Visa;
b) Carte d'achat MasterCard;
c) Dépôt direct (national et international);
d) Échange de données informatisées (EDI);
e) Virement télégraphique (international seulement);
f) Système de transfert de paiements de grande valeur (plus de 25 M$).

7.7.6 Vérification discrétionnaire

C0705C (2010-01-11), Vérification discrétionnaire des comptes

7.8 Instructions relatives à la facturation

a) 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 identifiés sur la facture soient complétés.

b) Chaque facture doit être appuyée par :

1. Une copie des feuilles de temps pour corroborer le temps de travail réclamé;
2. Une copie du document de sortie et de tout autre document tel qu'il est spécifié au contrat;
3. Une copie des factures, reçus.

b) Les factures doivent être distribuées comme suit :

1. une copie numérique doit être envoyé à l'adresse courriel suivante pour attestation et paiement : STG-CFSTG-J3-Fin@forces.gc.ca. Le numéro du contrat et le nom du responsable technique doivent être identifiés dans le sujet du courriel; et
2. une copie numérique doit être envoyé à l'autorité contractante par courriel identifiée sous l'article intitulé « Responsables » du contrat à l'adresse courriel suivante : tpsgc.facturation-zh.zh-invoicing.pwgsc@tpsgc-pwgsc.gc.ca. Le numéro du contrat et le nom de l'autorité contractante doivent être identifiés dans le sujet du courriel.

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 la province de l'Ontario, le Canada 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 2035 (2020-05-28), Conditions générales - besoins plus complexes de services;
c) Les conditions générales supplémentaires 4007 (2010-08-16), Le Canada détient les droits de propriété intellectuelle sur les renseignements originaux;
d) L'Annexe A, Énoncé des travaux;
e) L'Annexe B, Liste de vérification des exigences relatives à la sécurité;
f) L'Annexe C, Entente de non-divulgation; et
g) La soumission de l'entrepreneur datée du *à insérer au moment de l'attribution du contrat*

7.12 Contrat de défense

A9006C (2012-07-16), Contrat de défense

7.13 Ressortissants étrangers

A2000C (2006-06-16), Ressortissants étrangers (entrepreneur canadien) ou
A2001C (2006-06-16), Ressortissants étrangers (entrepreneur étranger)

7.14 Assurance

G1005C (2016-01-28), Assurances

7.15 Divulgation proactive de marchés conclus avec d'anciens fonctionnaires (s'il y a lieu)

En fournissant de l'information sur son statut en tant qu'ancien fonctionnaire touchant une pension en vertu de la *Loi sur la pension de la fonction publique* (LPFP) (https://laws-lois.justice.gc.ca/fra/lois/P-36/TexteComplet.html), 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 : 2012-2 du Secrétariat du Conseil du Trésor du Canada (https://www.canada.ca/fr/secretariat-conseil-tresor/services/avis-politique/2012-2.html).

7.16 Règlement des différends

a. Les parties conviennent de maintenir une communication ouverte et honnête concernant les travaux pendant toute la durée de l'exécution du marché et après.

b. Les parties conviennent de se consulter et de collaborer dans l'exécution du marché, 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 » (https://achatsetventes.gc.ca/pour-les-entreprises/vendre-au-gouvernement-du-canada/gestion-des-contrats/reglement-des-differends).

ANNEXE A, ÉNONCÉ DES TRAVAUX

1. TITRE

Outil d'évaluation des cyberopérateurs et formation de perfectionnement professionnel

2. OBJECTIF

L'objectif de cet énoncé des travaux (ÉDT) est de développer un outil d'évaluation de l'instruction et une trousse de formation de perfectionnement professionnel pour le Centre d'opérations des réseaux des Forces canadiennes (CORFC), afin de continuer à développer la profession de CYBEROP à l'appui des cyberopérations des FAC. Pour ce faire, un entrepreneur doit :

a. Développer, fournir et tenir à jour un outil d'évaluation professionnelle des cyberopérateurs (CYBEROP) par rapport au matériel de cours de qualification du grade (QG) de soldat (sdt) actuellement offert par le Willis College en vertu du contrat W4938-20069S/001/ZH; et
b. Élaborer et livrer une trousse de formation de perfectionnement professionnel (PP) correspondant au matériel du cours de la période de perfectionnement 1 (PP1) de la QG sdt.

3. CONTEXTE

3.1 En 2010, le vice-chef d'état-major de la Défense (VCEMD) a approuvé le groupe de travail sur la cybernétique, dont le mandat était d'établir et de mettre rapidement en place une nouvelle cybercapacité au sein des FAC. Ce mandat a ensuite été confié au directeur, Développement Forces opérationnelles Cyber (D DF Ops Cyber). La nécessité de former un effectif intégré et spécialisé pour mener des cyberopérations fait partie intégrante de ce mandat, ce qu'on a également approuvé en vertu de la Politique de défense du Canada - Protection, sécurité, engagement (PSE) en juin 2017. La politique PSE a fourni au ministère de la Défense nationale (MDN) et aux FAC un large éventail d'initiatives qui continueront de faire évoluer les capacités de combat du Canada, dont plusieurs sont directement liées à la guerre dans le domaine cybernétique, comme le développement et le perfectionnement de la force cybernétique des FAC, par la création d'une nouvelle profession de CYBEROP. Cette nouvelle profession a été créée et approuvée en 2017.

3.2 Les cyberspécialistes ont besoin d'une instruction individuelle et d'une éducation (II et E) considérables pour devenir efficaces; c'est ce principe directeur qui sous-tend le développement de cette nouvelle profession. Une composante importante de cette II et E est commune à celle qu'exigent les spécialistes en cybersécurité non militaires, d'autres aspects étant propres aux réseaux et aux systèmes du MDN et des FAC. Les défis associés à l'II et E dont les CYBEROP avancés ont besoin ont été mis en évidence au cours des études initiales et persistent encore aujourd'hui, notamment :

c. L'II et E spécifique à la profession de CYBEROP n'existe pas déjà pour les cyberopérations avancées au niveau requis pour cet ÉDT au sein des FAC;

d. À l'heure actuelle, les FAC ne disposent pas d'un cadre d'instructeurs à temps complet possédant le niveau d'éducation, de formation et d'expérience propres aux FAC et nécessaires pour développer, présenter et maintenir l'éventail complet d'II et E de CYBEROP avancé destiné au CYBEROP de niveau supérieur; et

e. Les exigences en matière d'infrastructures associées à toutes les facettes du nouveau programme de formation de CYBEROP dépassent la capacité de l'École d'électronique et des communications des Forces canadiennes (EECFC).

3.3 Au sein des FAC, la formation de CYBEROP a été confiée aux organisations suivantes :

a. L'EECFC est l'établissement d'instruction (EI) délégué chargé de former les stagiaires et de gérer ces derniers de manière individuelle. Le responsable technique (RT) peut désigner à sa discrétion une unité autre que l'EECFC; le cas échéant, il en avisera l'entrepreneur par courriel;

b. Le Groupe d'instruction de la génération du personnel militaire (GIGPM) est responsable de la gestion et de l'administration des programmes de formation. Le RT peut désigner à sa discrétion une unité autre que le GIGPM; le cas échéant, il en avisera l'entrepreneur par courriel;

c. Le directeur général du Développement des forces (Capacités d'information) (DGDFCI) est le RT et le principal point de contact pour l'entrepreneur. Le DGDFCI est chargé de conseiller l'EECFC et le GIGPM sur toutes les questions professionnelles et techniques touchant la profession de CYBEROP; et

d. Le Groupe des opérations d'information des Forces canadiennes (GOIFC) comprend les conseillers professionnels (CP) pour la profession de CYBEROP. Il a porté un besoin opérationnel urgent (BOU) à l'attention du CORFC pour s'assurer que les CYBEROP sont évalués en fonction de leurs compétences professionnelles actuelles.

3.4 En raison des défis décrits à la section 3.2 ci-dessus, le D DF Ops Cyber a accordé un contrat pour le cours de QG sdt CYBEROP dans le cadre du contrat W4938-20069S/001/ZH de TPSGC : formation d'une durée de 15 mois offerte au Willis College, dans la région de la capitale nationale (RCN). Il s'agit de la norme de base requise pour l'analyste de cyberdéfense. Comme cet ÉDT vise l'évolution de la formation de CYBEROP, on doit s'assurer que les CYBEROP sont compétents en vertu de la qualification QG sdt (PP1), leur permettant ainsi de progresser dans leur carrière pour obtenir la qualification QG PP2 de caporal-chef (cplc) pour des ensembles de compétences avancées en recherche de menaces.

4. ACRONYMES ET DOCUMENTS CONCERNÉS

4.1 Acronymes

Les acronymes suivants sont utilisés dans cet ÉDT :

FAC	Forces armées canadiennes
EECFC	École d'électronique et des communications des Forces canadiennes
CYBEROP	Cyberopérateur
DG	Directeur général
MDN	Ministère de la Défense nationale
DF	Développement des forces
TI	Technologie de l'information
II et E	Instruction individuelle et éducation
DISLI	Distribution limitée
QG cplc	Qualification de grade de caporal-chef
GIGPM	Groupe d'instruction de la Génération du personnel militaire
RCN	Région de la capitale nationale
OREN	Objectif de rendement
QG sdt	Qualification de grade de soldat
NQP	Normes de qualification et plans
SCCM	System Centre Configuration Management

PSE	Protection, sécurité, engagement
RT	Responsable technique
ÉI	Établissement d'instruction

4.2 Documents pertinents

Les documents suivants et toute modification à ceux-ci font partie intégrante de cet ÉDT dans la mesure indiquée aux présentes, et l'appuient :

a. Loi sur l'accès à l'information (https://laws.justice.gc.ca/fra/lois/a-1/index.html);
b. Loi canadienne sur l'accessibilité (https://www.parl.ca/DocumentViewer/fr/42-1/projet-loi/C-81/troisieme-lecture);
c. Loi sur les langues officielles (https://laws.justice.gc.ca/fra/lois/o-3.01/page-9.html);
d. Loi sur la protection des renseignements personnels (https://laws.justice.gc.ca/fra/lois/p-21/index.html);
e. Politique sur les marchés du Conseil du Trésor (https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=14494);
f. Lignes directrices du Secrétariat du Consil du Trésor sur les mesures d'accessibilité applicables aux marchés publics (en anglais seulement) (http://www.gcpedia.gc.ca/gcwiki/images/5/57/Accessibility_in_Procurement_Guidance_-_April_2019-V1%28EN%29.pdf);
g. Guide de développement du contenu du Réseau d'apprentissage de la Défense; https://www.canada.ca/en/department-national-defence/services/benefits-military/education-training/professional-development/defence-learning-network.html
h. Manuel d'instruction individuelle et d'éducation, série de publications A-P9-050-000/PT001 http://cda.mil.ca/pub/lib-bib/cfites-eng.asp
i. DOAD 5023-0, Universalité du service (https://www.canada.ca/fr/ministere-defense-nationale/organisation/politiques-normes/directives-ordonnances-administratives-defense/serie-5000/5023/5023-0-universalite-du-service.html);
j. DOAD 5039-0, Langues officielles (https://www.canada.ca/fr/ministere-defense-nationale/organisation/politiques-normes/directives-ordonnances-administratives-defense/serie-5000/5039/5039-0-langues-officielles.html);
k. DOAD 5039-4, Traduction de textes et obtention de documentation bilingue (https://www.canada.ca/fr/ministere-defense-nationale/organisation/politiques-normes/directives-ordonnances-administratives-defense/serie-5000/5039/5039-4-traduction-de-textes-et-obtention-de-documentation-bilingue.html);
l. National Defence Security Orders and Directives Chapter 6: Security of Information (http://national.mil.ca/en/health-safety-security/security-policies-ndsod.page);
m. ADM(IM) IT Security Policies and Standards (http://admim-smagi.mil.ca/en/security/policies-standards/index.page);
n. Appendice 1, Qualification de grade de soldat de cyberopérateur;
o. Appendice 2, Objectifs de rendement et objectifs de compétences pour la qualification de grade de soldat; et
p. Appendice 3, Liste des références pour la qualification du grade de soldat.

5. PORTÉE

5.1 La profession de CYBEROP nécessite un cheminement de carrière pour évoluer continuellement et acquérir une expérience approfondie en tant que CYBEROP en réponse aux incidents, aux opérations de l'équipe bleue, aux cyberopérations défensives (COD) et à la recherche avancée de menaces. Ce contrat vise à faciliter le perfectionnement professionnel de la profession de CYBEROP et à assurer qu'ils maintiennent leurs compétences PP1 avant de maîtriser les techniques avancées de chasse aux menaces PP2. L'outil d'évaluation et le programme de PP

sont nécessaires pour atténuer les risques contre le CYBEROP et représentent un impératif opérationnel pour le CORFC et les FAC. Ce contrat répondra, par conséquent, à un besoin opérationnel urgent (BOU) au sein du CORFC et sera utilisé chaque année pour évaluer les compétences des CYBEROP. Le RT aura besoin de temps pour passer en revue tout le contenu avant le premier cours pilote.

5.2 On s'attend à ce que le temps nécessaire pour offrir un programme de perfectionnement professionnel basé sur le matériel de cours de QG sdt de 15 mois soit de deux à trois mois, tout dépendant des résultats de l'outil d'évaluation. Cette exigence est nécessaire dans les 30 jours civils après avoir obtenu les résultats de l'outil d'évaluation.

6. EXIGENCES DE FORMATION

6.1 L'entrepreneur doit démontrer que son programme est agréé par un organisme de gouvernance et d'accréditation de l'enseignement supérieur du gouvernement provincial dans le domaine de l'analyse avancée de cyberdéfense (carrières civiles) ou des opérations de cybersécurité. L'entrepreneur doit :

a. Développer un outil d'évaluation pour évaluer les connaissances, les compétences et les qualités (CCQ) du CYBEROP en fonction des normes du cours de QG sdt de CYBEROP identifiées dans le contrat W4938-20069S/001/ZH, aux appendices 1, 2 et 3 de cet ÉDT, et fournir l'outil d'évaluation dans les 30 jours civils suivant l'attribution du contrat. Élaborer ensuite une trousse de formation de PP basée sur les résultats de l'outil d'évaluation par rapport à ce même matériel au personnel du CORFC (environ 48 personnes) pour répondre aux normes de la QG sdt et offrir la trousse de formation de PP dans les 30 jours civils suivant les résultats de l'outil d'évaluation;

b. Faire évaluer et approuver le matériel de cours élaboré (à l'exception des plans de cours) pour le module de formation de PP par le bureau du programme d'accréditation, de certification et d'équivalence des FAC (FAC-ACE) (http://www.caface-rfacace.forces.gc.ca/fr/index) avant de livrer la trousse de formation de PP aux stagiaires; ce qui peut prendre jusqu'à trois mois pour que les FAC-ACE évaluent et approuvent le matériel de cours. Afin de se connecter, l'entrepreneur doit s'inscrire pour obtenir un compte de FAC-ACE. Si l'entrepreneur a des problèmes, il doit communiquer avec l'administrateur du système FAC-ACE;

c. Tenir à jour ce programme de formation de PP abrégé, y compris tout le matériel de cours (plans de cours, manuels, évaluations et cahiers d'exercices, etc.) et les travaux pratiques en laboratoire, qui répondront aux objectifs de rendement (OREN) 001 à 005 de la QG sdt de CYBEROP énoncés dans le contrat W4938 -20069S/001/ZH aux appendices 1 à 3 de cet ÉDT. Pour tenir ce contrat à jour, tout le matériel de cours doit faire l'objet d'un examen tous les deux ans par la cellule des normes de l'ÉI, ou le matériel de cours doit remonter à moins de deux ans pour correspondre aux pratiques exemplaires modernes en matière de cybersécurité;

d. Préparer des évaluations pratiques et théoriques du cours pour tous les contrôles afin d'assurer qu'ils ont répondu aux exigences visant chaque stagiaire, comme l'indique l'outil d'évaluation. Elles consistent en contrôles de compétences (COCOM) pour aider le personnel enseignant et les apprenants à mesurer les progrès afin de confirmer le processus d'apprentissage ou pour cerner les domaines qui doivent faire l'objet de mesures correctives, et en contrôles de rendement (COREN) pour établir la réussite des apprenants au module de formation de PP.

e. En ce qui concerne la trousse de formation de PP, soumettez toutes les modifications au matériel de cours (à l'exception des plans de cours) pour évaluation et approbation par le bureau du programme de la cellule responsable des normes de l'ÉI.

6.2 L'entrepreneur doit être en mesure de donner 37,5 heures d'enseignement par semaine de 12 stagiaires et jusqu'à un maximum de 24 participants par classe, et d'assurer que les heures établies de la journée de formation standard sont respectées selon le calendrier convenu. Si l'entrepreneur considère les devoirs comme une partie essentielle du programme de cours, cela sera acceptable aux yeux du RT. L'entrepreneur doit convenir du calendrier avec le CORFC et le RT en fonction des tâches opérationnelles du CORFC et peut inclure le travail du soir, le travail par quarts ou la formation en fin de semaine. Le calendrier d'instruction hebdomadaire doit comprendre :

a. 27,5 heures de théorie (temps d'apprentissage programmé);
b. Cinq périodes d'une heure pour le dîner;
c. Trois périodes d'une heure pour l'entraînement physique (au début ou à la fin de la journée d'instruction); et
d. Une période d'administration personnelle de deux heures.

6.3 L'entrepreneur doit être agréé par une autorité scolaire canadienne reconnue par la province en tant qu'établissement décernant des diplômes d'études postsecondaires. L'entrepreneur doit conserver cette reconnaissance pendant toute la durée du contrat.

6.4 L'entrepreneur doit fournir un site et des installations d'instruction situés à l'intérieur des limites géographiques de Kingston, en Ontario ou dans la RCN. Le contrat doit assurer que les membres des FAC auront accès gratuitement à un stationnement. Si l'enseignement en personne n'est pas possible en raison des restrictions liées à la COVID-19, l'entrepreneur devra donner tous les cours de manière virtuelle et prévoir des périodes avec l'instructeur en personne et s'assurer que les cyberlaboratoires et les exercices d'instruction collective sont pris en charge. L'entrepreneur doit s'assurer que tous les stagiaires possèdent l'équipement de TI nécessaire pour suivre la formation de PP.

6.5 Le gouvernement du Canada s'efforce d'assurer que les biens et services qu'il achète sont inclusifs de par leur conception et accessibles par défaut, conformément à la Loi canadienne sur l'accessibilité, aux règlements et aux normes connexes, ainsi qu'à la Politique sur les marchés du Conseil du Trésor. Le personnel militaire doit être en bonne condition physique, apte au travail et déployable pour aller effectuer des tâches opérationnelles générales (DOAD 5023-0, Universalité du service).

7. MÉTHODOLOGIE DE FORMATION

7.1 L'entrepreneur doit développer un outil d'évaluation et évaluer tout le personnel du CORFC en vertu des normes de cours PP1 de la QG sdt. L'entrepreneur doit ensuite élaborer et offrir des trousses de formation de PP individuelles pour répondre aux exigences mises en évidence dans l'outil d'évaluation. Cette trousse doit être souple pour permettre de travailler virtuellement avec les stagiaires pendant les périodes de service opérationnel.

7.2 L'entrepreneur doit incorporer des sessions pratiques durant la formation pour accroître les compétences des stagiaires dans l'utilisation des logiciels courants d'analyste de réseau dans les secteurs publics/privés et des logiciels couramment utilisés par les CYBEROP des FAC. Les postes de travail et serveurs Linux et Windows sont un exemple de système d'exploitation type. Les logiciels comprennent Apache, PHP, MySQL, Adobe, Microsoft Office et Wireshark. En plus des systèmes d'exploitation énumérés ci-dessus, l'entrepreneur doit également intégrer au matériel de cours des interpréteurs de scripts comme Python et Ruby, des outils d'analyse de maliciels comme Cuckoo Sandbox et des utilitaires de configuration comme System Center Configuration Management (SCCM), comme le mentionne l'EECFC.

7.3 L'entrepreneur doit s'assurer que tous les examens, le matériel et la formation sont disponibles dans les deux langues officielles du Canada et remis ou présentés aux stagiaires dans la langue de leur choix.

7.4 L'entrepreneur doit offrir une formation conforme aux pratiques et aux normes des collèges communautaires de la province, telles que déterminées par l'autorité d'approbation de l'éducation reconnue par la province (comme le Conseil des universités de l'Ontario).

7.5 L'entrepreneur doit appliquer les procédures, les normes et les pratiques d'évaluation académique des étudiants des collèges communautaires approuvées par la province. L'entrepreneur doit aviser dès que possible le RT de tout stagiaire qui risque d'être incapable d'avancer dans le programme ou de le réussir, et ce avant la fin du cours et avant son retrait du programme. Le RT examinera la situation académique du stagiaire et acheminera par courriel toute disposition nécessaire à l'entrepreneur. Le RT peut diriger les évaluations supplémentaires des stagiaires, comme demander un deuxième avis ou leur donner une autre chance de s'améliorer.

7.6 La cellule des normes de l'EFCFC peut surveiller toutes les séances d'instruction et d'évaluation en avisant par écrit l'entrepreneur au préalable. Les commentaires en découlant seront envoyés par courriel à l'entrepreneur et au RT.

7.7 L'entrepreneur doit au besoin fournir une assistance à l'instruction conformément aux procédures convenues par écrit avec l'EECFC, soit jusqu'à cinq séances d'une heure par semaine. Ces dispositions doivent être présentées à l'EECFC au moins 30 jours ouvrables avant le début du programme. L'entrepreneur ou l'EECFC peut modifier ces modalités, pourvu qu'ils se consultent et que l'autre partie ait confirmé son consentement par courriel.

7.8 À la demande du RT, l'entrepreneur doit fournir une copie de tous les documents notés des stagiaires. Les documents sensibles du point de vue académique doivent être protégés de la manière décrite au chapitre 6 des ODSDN (section 4.2 (m) ci-dessus).

7.9 L'entrepreneur doit fournir au RT le relevé de notes final de chaque stagiaire dans les 30 jours ouvrables suivant son départ ou la fin du programme de formation. Les relevés de notes des stagiaires doivent être protégés de la manière décrite à la section 4.2 (m).

8. CALENDRIER DE FORMATION

8.1 À une date d'attribution du contrat mutuellement convenue, l'entrepreneur doit fournir au RT une copie électronique de l'application de l'outil d'évaluation de la QG sdt (PP1) et de la trousse de formation de PP en format Microsoft Word ou Excel. L'entrepreneur doit collaborer avec le RT afin de préciser le calendrier proposé pour répondre à la demande opérationnelle du personnel du CORFC.

8.2 Le programme de formation préliminaire doit indiquer clairement la liste de toutes les séances d'apprentissage pratiques et théoriques. Aux fins de planification initiale, l'horaire quotidien devrait commencer à 8 h 00 et se terminer à 16 h 00. Si des restrictions liées à la COVID sont en place, l'entrepreneur doit faire appel à d'autres méthodes d'apprentissage virtuel, conformément à la section 6.4 ci-dessus.

9. SITE DE FORMATION ET SOUTIEN ADDITIONNEL

9.1 L'entrepreneur doit fournir un site de formation et des installations conformes aux pratiques et aux normes des collèges communautaires de l'Ontario pour ce type de programme d'apprentissage. La salle de classe ou le laboratoire informatique doit accueillir tous les stagiaires, le mobilier, le matériel ainsi que tout le matériel informatique (TI) et les logiciels communs nécessaires pour répondre aux exigences de formation de PP de la QG sdt (PP1). Si l'enseignement en personne est impossible en raison des restrictions liées à la COVID-19, l'entrepreneur doit fournir virtuellement toutes les instructions de travail théoriques et pratiques en laboratoire avec des périodes d'instruction en direct intégrées, conformément à la section 6.4 ci-dessus.

9.2 L'entrepreneur doit donner accès au site et aux installations de formation au besoin pour apporter un soutien supplémentaire à la formation et assurer les pratiques des stagiaires (supervisées ou non) en dehors de la journée de cours standard.

9.3 L'entrepreneur doit fournir une seule copie papier de tout manuel ou matériel didactique (trousse de formation de PP) à chaque stagiaire et au moins une copie papier à l'ÉI. Les manuels achetés par le MDN resteront la propriété du MDN.

9.4 L'entrepreneur doit fournir tout le matériel didactique consommable. Cela comprend, entre autres, les manuels et les documents de cours. Cela ne comprend pas les fournitures d'apprentissage consommables de chaque stagiaire (c'est-à-dire le matériel qui peut varier d'un stagiaire à l'autre et qu'ils peuvent utiliser pour faciliter leur apprentissage, comme papier, stylos, crayons, articles de papeterie, etc.).

9.5 L'entrepreneur doit fournir l'accès à la salle de classe ou au laboratoire informatique à tous les stagiaires, incluant le matériel informatique périphérique et l'accès voulu au réseau de support d'information.

9.6 L'entrepreneur doit fournir aux apprenants l'équipement informatique, les ressources de soutien et un réseau offrant un accès à l'Internet, des comptes de courriel individuels pour les stagiaires avec 1 Go (minimum) de stockage pour le courriel, un compte Web avec 5 Go (minimum) d'espace disque et un accès à distance au réseau de l'entrepreneur. La salle de classe ou le laboratoire informatique doit inclure tout le matériel informatique nécessaire pour présenter une formation répondant aux exigences de formation de CYBEROP sur les trousses de PP, et elle doit inclure des systèmes de sauvegarde réseau appropriés pour assurer l'intégrité des données et du travail des stagiaires.

9.7 Le matériel doit être géré selon un cycle de vie maximal de quatre ans, aux frais de l'entrepreneur.

9.8 À la fin du programme de formation, tout équipement informatique loué (comme les ordinateurs portables, disques durs, etc.) doit être nettoyé et/ou retourné à un tiers conformément aux politiques et normes de sécurité informatique du SMA (GI), conformément à la section 4.2 (n).

9.9 Pour appuyer les objectifs de formation, l'entrepreneur doit mettre en place un serveur et une infrastructure de réseau conformes aux exigences canadiennes en matière de traitement et de stockage des renseignements personnels des membres des FAC, décrites dans les ordonnances et directives de sécurité de la Défense nationale, chapitre 6 - Sécurité de l'information (voir la section 4.2 (m)). L'entrepreneur et tout membre de son personnel devant accéder aux renseignements personnels des apprenants doit remplir et signer l'entente de confidentialité.

9.10 L'entrepreneur doit répondre aux exigences habituelles visant les salles de classe et l'informatique énumérées dans les NQP PP1 de QG sdt, et installer dans la salle de classe ou le laboratoire informatique les logiciels suivants :

a. Systèmes d'exploitation standard de l'industrie (comme les systèmes client et serveur LINUX/Windows);
b. Logiciels standard de l'industrie (comme Apache, PHP, MySQL, Adobe, Microsoft Office et Wireshark);
c. Interpréteurs de script standard de l'industrie (comme Python et Ruby);
d. Outils d'analyse de maliciels standard de l'industrie (commeCuckoo, Sandbox et InetSim), et
e. Logiciel de configuration (comme SCCM).

9.11 L'entrepreneur doit coordonner les mises à jour aux logiciels. Il lui incombe de déterminer l'échéancier optimal de ces mises à jour afin de perturber les cours le moins possible et coordonner les modifications des plans de cours en fonction du matériel pédagogique disponible lié à la plus récente version du logiciel. On entend par mise à jour toute modification ou tout correctif à un logiciel où l'entier du numéro de version reste inchangé.

9.12 L'entrepreneur doit acheminer au RT par courriel une preuve des ententes ou des licences visant les logiciels ou le matériel dans les 30 jours civils avant le début du programme de formation.

9.13 L'entrepreneur doit prévoir des bureaux adaptés aux visites du personnel de l'ÉI, y compris des bureaux à occupation simple pour deux membres du personnel, plus une salle privée pour des consultations ou des entrevues. Les bureaux doivent être meublés conformément aux pratiques et aux normes en vigueur pour le personnel enseignant dans les collèges communautaires de l'Ontario. Les bureaux doivent comprendre au moins deux téléphones individuels et un accès aux lignes de communication de données. L'accès à ces installations par les stagiaires doit être assuré au besoin, pour apporter un soutien supplémentaire et leur permettre de pratiquer hors des heures de formation prévues.

9.14 L'entrepreneur doit prévoir un réfrigérateur pour y ranger pendant la journée les repas des stagiaires en toute sécurité . Ce réfrigérateur doit pouvoir contenir les repas d'au plus 24 stagiaires, à raison de deux repas par jour.

9.15 L'entrepreneur doit fournir un four à micro-ondes pour permettre aux stagiaires de réchauffer leur repas sans danger.

9.16 L'entrepreneur doit fournir une salle à manger distincte de la salle de classe ou du laboratoire informatique où les stagiaires pourront prendre leurs repas en groupe. La salle doit être suffisamment grande pour accueillir tous les apprenants censés prendre leur repas en même temps (s'il n'y a qu'une seule période de repas, tous les élèves devraient pouvoir le prendre en même temps dans cette salle).

9.17 L'entrepreneur doit fournir un photocopieur (et notamment du papier de différentes tailles, du toner et des cartouches d'encre) à l'intention des stagiaires, sans frais pour eux ni pour le Canada.

10. BESOINS EN MATIÈRE DE RESSOURCES HUMAINES

10.1 Pour mettre en place le programme de formation de CYBEROP et répondre pleinement aux exigences connexes, l'entrepreneur doit fournir les ressources suivantes, notamment :

a. Un superviseur des contrats, qui s'occupera de gérer les contrats et les questions connexes;
b. Un coordonnateur de programme, pour assurer la mise en œuvre du programme et la supervision des ressources embauchées à forfait;
c. Des instructeurs qualifiés, dans une proportion d'un instructeur pour 12 stagiaires;
d. Un ou plusieurs technicien(s) en informatique, pour assurer la maintenance des systèmes de support informatique et le soutien technique à l'intention des stagiaires. Le temps de formation perdu en raison de défaillances techniques, de la maintenance du système informatique ou de toute circonstance imprévue doit être repris par l'entrepreneur sans frais supplémentaires pour le Canada afin de garantir que les heures d'enseignement données chaque semaine aux stagiaires sont dispensées conformément à la section 6.2.

10.2 Compétences obligatoires minimales

Les ressources de l'entrepreneur doivent satisfaire aux qualifications obligatoires minimales pour leur catégorie de ressources respective :

a. Les professeurs qualifiés de la faculté doivent posséder :
   i. Au moins quatre années d'expérience; et
   ii. Une maîtrise en informatique, en programmation informatique, en science de l'information ou en génie informatique d'une université, d'un collège ou d'une école secondaire reconnu au Canada, ou l'équivalent, établi par un service canadien reconnu d'évaluation des attestations d'études (https://www.cicdi.ca/1/accueil.canada), si elles ont été obtenues à l'extérieur du Canada;

b. Les instructeurs ou aides-enseignants doivent posséder :
   i. Au moins trois années d'expérience en formation dans un domaine lié aux OREN et aux OCOM connexes à l'appendice 1; et
   ii. Un baccalauréat en informatique, en programmation informatique, en science de l'information ou en génie informatique d'une université, d'un collège ou d'une école secondaire reconnu au Canada, ou l'équivalent établi par un service canadien reconnu d'évaluation des attestations d'études (https: // www .cicic.ca/2/home.canada), si elles ont été obtenues à l'extérieur du Canada.

11. COMPÉTENCES LINGUISTIQUES

11.1 L'entrepreneur et ses ressources doivent maîtriser (compréhension et expression orales, lecture, écriture) une des langues officielles du Canada (anglais ou français), ou les deux; la maîtrise équivaut au niveau 8 des Canadian Language Benchmarks pour l'anglais et des Niveaux de compétence linguistique canadiens pour le français : https://www.language.ca/overview-of-clb-and-nclc-competency-levels/.

11.2 L'entrepreneur doit avoir un processus d'assurance-qualité établi incluant la correction d'épreuves pour la correspondance et les produits livrables en anglais et en français.

11.3 Le Canada se réserve le droit de demander à l'entrepreneur d'évaluer la compétence linguistique de ses ressources pendant toute la durée du contrat, sans frais supplémentaires pour le Canada, au moyen d'un des tests linguistiques approuvés par Immigration, Réfugiés et Citoyenneté Canada. Si une évaluation du personnel de l'entrepreneur révèle qu'une ressource ne répond pas aux exigences linguistiques, l'entrepreneur doit immédiatement la remplacer sans frais supplémentaires pour le Canada.

12. RÉUNIONS

Les dépenses de l'entrepreneur et de ses ressources liées aux réunions ne seront pas remboursées.

12.1 Réunion initiale

Une réunion initiale doit avoir lieu dans les cinq jours ouvrables suivant l'attribution du contrat. Cette réunion doit se tenir dans l'ÉI, au CCRFC ou par conférence téléphonique. L'heure et l'emplacement exacts de cette réunion seront convenus par l'entrepreneur et le RT.

b. La réunion initiale servira à :
   i. Revoir les exigences contractuelles;
   ii. Revoir et clarifier, au besoin, les responsabilités et les rôles respectifs de l'EECFC, du CORFC, du RT et de l'entrepreneur pour éviter tout malentendu; et
   iii. Revoir et clarifier le calendrier d'évaluation des stagiaires au moyen de l'outil d'évaluation.

12.2 Réunions mensuelles

a. Le superviseur de contrat et le coordonnateur de programmes de l'entrepreneur doivent participer à des réunions d'orientation de la formation dans la RCN ou à Kingston ou par conférence téléphonique avec le RT, l'EECFC et le COFCFC, pour se pencher sur l'état de la formation et la progression des stagiaires. Ces réunions d'orientation de la formation n'auront pas lieu plus d'une fois par mois civil, à moins d'une entente entre l'entrepreneur et l'ÉI. La date et l'heure des réunions mensuelles feront l'objet d'un accord mutuel entre l'entrepreneur et le RT.

L'entrepreneur est chargé de préparer les ordres du jour et les comptes rendus de toutes les réunions. Les ordres du jour doivent être disponibles cinq jours ouvrables avant les réunions, et l'ébauche des comptes rendus doit être remise au RT pour examen dans les trois jours ouvrables suivant la réunion.

13. RESTRICTIONS

13.1 Les décisions portant sur la révision ou la définition de la politique, des budgets ainsi que des obligations contractuelles et des exigences ne font pas partie des services de l'entrepreneur. Les ressources de l'entrepreneur doivent seulement formuler des commentaires et des recommandations à l'intention du RT à ce sujet.

13.2 Les employés de l'entrepreneur qui fournissent des services ne doivent pas relever directement de fonctionnaires fédéraux et ne doivent en aucun cas être des employés ou des fonctionnaires au gouvernement du Canada.

13.3 Pendant l'exécution du contrat, l'entrepreneur ou ses employés ne doivent diriger aucune organisation ministérielle ou aucun personnel de tiers avec lequel le Canada a passé, ou compte passer, un contrat en vue de l'exécution d'activités.

13.4 En tout temps pendant la prestation des services demandés, les employés de l'entrepreneur ne doivent pas avoir accès à des renseignements exclusifs, notamment des renseignements financiers (notamment prix et tarifs unitaires) ou techniques sur un tiers avec lesquels le Canada a conclu, ou compte conclure, un contrat, sauf aux renseignements de domaine public, comme la valeur totale des marchés attribués. Les employés de l'entrepreneur peuvent obtenir des renseignements exclusifs dans le cadre de la prestation des services s'ils ont dûment rempli et signé l'entente de confidentialité.

13.5 Tous les dessins, codes logiciels, rapports, données, documents ou matériaux fournis à l'entrepreneur par le Canada ou produits par le personnel de l'entrepreneur dans le cadre du contrat doivent être utilisés uniquement pour combler le besoin faisant l'objet du contrat. L'entrepreneur doit protéger les informations et les documents énoncés ci-dessus contre toute utilisation non autorisée et il ne doit les transmettre à aucun tiers, personne ou organisation à l'extérieur du MDN sans avoir obtenu la permission écrite expresse de l'organisation visée ou du RT. Ces renseignements et ce matériel doivent être remis à cette organisation ou au RT une fois les services rendus, ou à la demande du RT.

13.6 Toute la correspondance produite par les employés de l'entrepreneur ou par une section du MDN doit être présentée à l'organisation visée ou au RT. La correspondance comprend les enregistrements des conversations, les comptes rendus des décisions et la correspondance écrite, peu importe son format.

13.7 Le RT ou l'organisation touchée aura accès en tout temps aux travaux et aux installations où toute partie des travaux est exécutée.

13.8 L'entrepreneur doit s'assurer que son personnel n'utilise pas les désignations, logos ou insignes du gouvernement du Canada ou du MDN sur ses cartes professionnelles, écriteaux de bureau ou de poste de travail ni dans sa correspondance électronique ou écrite afin de ne pas donner l'impression qu'il fait partie des employés du gouvernement du Canada.

Appendice 1

Qualification de grade de soldat cyberopérateur

Liste des abréviations

CYBEROP	Cyberopérateur
QG sdt	Qualification de grade de soldat
OREN	Objectif de rendement
OCOM	Objectif de compétence
MDN	Ministère de la Défense nationale
FAC	Forces armées canadiennes
TI	Technologie de l'information
SDI	Système de détection d'intrusion
SPI	Système de protection contre les intrusions
IP	Protocole Internet
SE	Système d'exploitation
DPI	Dirigeant principal de l'information
OSSI	Officier de sécurité des systèmes d'information
EVC	Expositions et vulnérabilités communes
Réf.	Référence
DNS	Serveur de noms de domaine
DHCP	Protocole DHCP
IIS	Internet Information Server
LAMP	Linux, Apache, MySQL et PHP

Aperçu des besoins en matière d'instruction : Les cyberopérateurs (CYBEROP) effectuent des opérations de défense de réseaux informatiques et assurent une liaison avec les alliés du Canada afin d'améliorer les capacités du ministère de la Défense nationale (MDN) et des Forces armées canadiennes (FAC) pour mettre en place un environnement informatique sécuritaire. Ils surveillent les réseaux de communication des FAC afin de déceler toute tentative d'accès non autorisé au réseau et d'intervenir face à celle-ci. Ils fournissent aussi un appui cybernétique afin de combler les besoins opérationnels de la Marine, de l'Armée de terre et de la Force aérienne. Les activités et les tâches cybernétiques offensives, qui comprennent la perturbation des actions des adversaires dans le cyberdomaine, entrent aussi dans leur travail. Cette instruction vise à préparer les cyberopérateurs à effectuer les tâches de l'emploi de premier échelon de « CYBEROP ». Les fonctions sont exercées dans un centre d'opérations en appui à des éléments maritimes, terrestres et aériens. La principale responsabilité est d'identifier des indicateurs de compromission par l'analyse des réseaux du MDN et des FAC. Les tâches principales consistent à rassembler, examiner et analyser les cyberalertes, et produire des rapports techniques à leur sujet.

Aperçu de la stratégie d'instruction : Ceci est une nouvelle exigence d'instruction (c.-à-d., aucune version des FAC de ce cours n'est donnée). Le programme d'instruction est divisé en deux éléments principaux :

Module 1 – OREN 001 à 005 (principal objectif de cette exigence d'instruction, présentée ci-dessous) : doit être donné par l'entrepreneur.

Module 2 – OREN 006 et 007 (ne sont pas inclus dans la présente exigence d'instruction) : doit être donné par un établissement d'instruction des FAC. L'objectif de ces OREN est de préparer le cyberopérateur à mettre en application les compétences génériques et les techniques de surveillance du réseau élaborées dans les OREN 001 à 005 dans le contexte des FAC.

OREN et OCOM connexes :

OREN 001 – Maintenir une connaissance de la situation du réseau : Cet OREN vise à préparer le CYBEROP à mener des activités visant à établir et maintenir une connaissance de la situation de la structure, de la composition, des habitudes de trafic et de la posture de sécurité d'un réseau. Cet objectif est atteint par l'utilisation d'outils automatisés, de méthodes manuelles et de divers niveaux d'analyse des données brutes. En énumérant le réseau, en créant la carte du réseau et en étalonnant le trafic du réseau, le CYBEROP doit bien connaître les technologies, l'architecture, les appareils et les communications du réseau. Pour être en mesure d'évaluer les vulnérabilités, il doit connaître les vulnérabilités, les menaces et les vecteurs d'attaque courants afin de les analyser et donner des conseils sur les mesures d'atténuation. De plus, il doit avoir une compréhension générale des divers SE (ordinateur et serveur), de la virtualisation et des divers autres domaines de la réseautique et des TI afin de détecter toute anomalie dans une analyse de réseau ou d'une capture de paquets.

OCOM 001.01 — Énumérer un réseau et un système
OCOM 001.02 — Développer une carte de réseau logique
OCOM 001.03 — Cerner les vulnérabilités du réseau et du système
OCOM 001.04 — Caractériser le trafic du réseau pour déterminer les habitudes normales

OREN 002 – Réagir à un cyberévénement : Cet OREN vise à préparer le CYBEROP à enquêter sur un événement au moyen de données recueillies à l'aide d'un ensemble d'outils de cyberdéfense (p. ex., alertes SDI, pare-feu, registres du trafic du réseau). L'analyste franchit les étapes pour analyser l'événement qui s'est produit dans son environnement afin d'atténuer les menaces par l'entremise de rapports internes.

OCOM 002.01 — Détecter une activité qui représente une menace
OCOM 002.02 — Enquêter sur des cyberévénements
OCOM 002.03 — Produire des rapports internes
OCOM 002.04 — Préserver les preuves scientifiques de cybercriminalité

OREN 003 – Produire un rapport technique : Cet OREN vise à préparer le CYBEROP à produire un rapport à partir de toutes les données brutes disponibles, à réaliser les analyses et les autres rapports pertinents et les autres intrants relatifs au cyberespace.

OCOM 003.01 — Regrouper des données pertinentes pour produire un rapport technique
OCOM 003.02 — Produire un rapport technique
OCOM 003.03 — Produire un rapport technique pour une distribution orale ou écrite

OREN 004 – Préparer un environnement d'analyse : Cet OREN vise à préparer le CYBEROP à configurer le matériel et les logiciels. Le CYBEROP sera capable d'installer, de maintenir et de retirer le matériel et les logiciels de cyberdéfense, et de créer et retirer des règles de SDI/SPI. La préparation et la configuration de divers appareils de sécurité dans un environnement de petit réseau prépareront le cyberopérateur aux applications personnalisées et aux exigences de déploiement particulières. À l'appui des sciences judiciaires et de l'analyse de logiciels malveillants des FAC, le cyberopérateur doit posséder une compréhension pratique des plateformes virtuelles.

OCOM 004.01 — Installer le matériel requis
OCOM 004.02 — Configurer les dispositifs de sécurité du réseau physique
OCOM 004.03 — Préparer et mettre sur pied des systèmes d'exploitation virtuels
OCOM 004.04 — Configurer un logiciel
OCOM 004.05 — Faire le dépannage des défaillances matérielles des outils
OCOM 004.06 — Faire le dépannage des défaillances logicielles des outils
OCOM 004.07 — Installer et mettre à jour les capteurs du réseau
OCOM 004.08 — Retirer les logiciels et le matériel nécessaire

OREN 005 – Développer des outils logiciels : Cet OREN vise à préparer le CYBEROP à concevoir, créer, tester et maintenir des outils logiciels personnalisés. Il pourra déterminer les défaillances des outils existants afin de concevoir et créer des outils pour résoudre ces défaillances. Il doit posséder des compétences en création de scripts et doit pouvoir écrire de petits programmes afin de créer des outils personnalisés. Cet OREN n'a pas pour objectif de faire du cyberopérateur un expert en développement de logiciels, mais il lui permettra d'acquérir des compétences de base en création de scripts et des compétences de base pour les autres OREN, ainsi que pour des instructions spécialisées futures pour des postes.

OCOM 005.01 – Planifier le développement des outils logiciels
OCOM 005.02 – Concevoir des outils logiciels
OCOM 005.03 – Concevoir des outils logiciels

Appendice 2

Objectifs de rendement et objectifs de compétence
Pour la qualification du grade de soldat

Voir l'appendice 3 pour une liste des références aux OCOM codés de façon alphanumérique (C1, C2, C3, etc.) pour la qualification de grade de soldat.

OREN 001 – Maintenir une connaissance de la situation du réseau

OCOM	Contenu de l'OCOM (ce que les stagiaires doivent être capables de faire à la fin de l'éducation et de l'instruction connexes)
OCOM 001.01 – Énumérer un réseau et un système	(1) Préparer l'outil d'analyse du réseau, ce qui consiste à : (a) préciser les objectifs et l'espace du protocole Internet (IP); (b) vérifier les objectifs et l'espace IP comme une propriété du MDN/FAC; (c) configurer l'outil d'analyse réseau, conformément aux documents sur l'outil. (2) Faire l'essai d'une fonction d'évaluation de réseau personnalisée, ce qui consiste à : (a) lancer l'outil avec les configurations actuelles sur une plage IP d'essai; (b) valider le résultat du test pour s'assurer que les résultats sont corrects; (c) régler les configurations de l'analyse, au besoin, pour tenir compte des problèmes imprévus visant l'utilisation de la bande passante, la durée d'exécution de l'analyse ou d'autres paramètres. (3) Utiliser un outil d'analyse réseau sur un espace IP ciblé, ce qui consiste à : (a) lancer le balayage et en surveiller la progression; (b) dépanner la progression de l'analyse et en assurer la reconfiguration, ce qui comprend la pause, l'évaluation des résultats, la modification et la reprise; (c) valider le résultat de l'analyse pour s'assurer que les résultats sont corrects; (d) traiter le résultat, afin d'obtenir un format lisible ou une image. (4) Analyser les résultats de l'analyse, ce qui consiste à : (a) cerner les informations critiques, ce qui consiste à : i. nommer les applications et les systèmes d'exploitation (SE) d'un dispositif; et ii. cerner d'autres informations, notamment le type de dispositif, l'état du port, l'adresse IP, le nom de l'hôte, etc.; (b) prendre les empreintes numériques du dispositif, ce qui consiste à : i. caractériser le dispositif en regroupant les éléments d'identification, ii. valider la prise d'empreintes, au besoin, par des analyses de confirmation, des outils secondaires ou d'autres sources d'information; (c) déterminer l'emplacement des ressources physiques du réseau, ce qui consiste à :

OCOM	Contenu de l'OCOM (ce que les stagiaires doivent être capables de faire à la fin de l'éducation et de l'instruction connexes)
	i. désigner l'emplacement à l'aide d'outils automatisés (p. ex., IP Control) ou d'autres outils de surveillance du réseau, ii. désigner l'emplacement à l'aide d'autres méthodes, comme vérifier la géolocalisation d'autres adresses IP à l'intérieur de la portée et faire la corrélation avec des données d'analyse antérieures et d'autres dispositifs identifiés ou d'autres renseignements. (5) Mettre à jour la base de données de connaissance de la situation du réseau conformément au mode d'exploitation de la base de données et aux documents.
OCOM 001.02 – Développer une carte de réseau logique	(1) Recueillir de l'information sur les ressources du réseau, ce qui comprend les données relatives : (a) au trafic sur le réseau; (b) à la numérisation automatisée; et (c) aux organisations partenaires. (2) Créer une carte de réseau, ce qui comprend l'utilisation de : (a) méthodes manuelles (p. ex., Microsoft Visio, Microsoft PowerPoint) ou d'autres moyens; et (b) méthodes automatisées, ce qui comprend des outils (p. ex., ZenMap, LanState Pro) et des scripts. (3) Mettre à jour la base de données de connaissance de la situation du réseau conformément au mode d'exploitation de la base de données et aux documents.
OCOM 001.03 – Cerner les vulnérabilités du réseau et du système	(1) Préparer des outils d'évaluation des vulnérabilités et une méthodologie d'évaluation, ce qui consiste à : (a) évaluer l'ensemble de services et la documentation du client; (b) identifier les objectifs, l'espace IP et la portée de l'analyse; (c) confirmer que les objectifs et l'espace IP sont propriété du MDN/des FAC; (d) acquérir les droits administratifs ou l'équivalent pour atteindre les résultats de l'analyse; et (e) configurer l'outil d'évaluation des vulnérabilités, conformément aux documents sur l'outil. (2) Faire l'essai d'une fonction d'évaluation de réseau personnalisée, ce qui consiste à : (a) lancer l'outil avec les configurations actuelles sur une plage IP d'essai; (b) valider le résultat du test pour s'assurer que les résultats sont corrects; (c) régler les configurations de l'analyse, au besoin, pour tenir compte des problèmes imprévus visant l'utilisation de la bande passante, la durée d'exécution de l'analyse ou d'autres paramètres. (3) Procéder à une évaluation de la vulnérabilité fondée sur des outils, ce qui consiste à : (a) lancer le balayage et en surveiller la progression; (b) dépanner la progression de l'analyse et en assurer la reconfiguration, ce qui comprend la pause, l'évaluation des résultats, la modification et la reprise; (c) valider le résultat de l'analyse pour s'assurer que les résultats sont corrects;

OCOM	Contenu de l'OCOM (ce que les stagiaires doivent être capables de faire à la fin de l'éducation et de l'instruction connexes)
	(d) traiter le résultat, afin d'obtenir un format lisible ou une image. (4) Effectuer une évaluation de la vulnérabilité fondée sur des outils, ce qui consiste à : (a) assurer la liaison avec des experts en la matière, des administrateurs de systèmes, des opérateurs de systèmes, les ressources techniques, les DPI/OSSI et d'autres intervenants; (b) évaluer la configuration et les processus des réseaux par rapport aux pratiques exemplaires et aux normes de l'industrie; (c) appuyer le responsable de la tâche en évaluant les contrôles de sécurité, y compris la sécurité physique, procédurale, personnelle et de la TI du réseau ou du système. (5) Analyser les résultats de l'évaluation de vulnérabilité manuelle et automatisée, ce qui consiste à : (a) examiner les cotes de gravité des résultats automatisés (p. ex., codes CVE); (b) évaluer ensemble les résultats manuels et automatisés; et (c) évaluer l'incidence et la probabilité d'exploitation de toutes les vulnérabilités découvertes. (6) Produire des rapports. (7) Mettre à jour la base de données de connaissance de la situation du réseau conformément au mode d'exploitation de la base de données et aux documents.

OCOM	Contenu de l'OCOM (ce que les stagiaires doivent être capables de faire à la fin de l'éducation et de l'instruction connexes)
OCOM 001.04 – Caractériser le trafic du réseau pour déterminer les habitudes normales	(1) Se préparer pour la collecte de données sur le trafic, ce qui consiste à : (a) désigner les dispositifs du réseau et les dispositifs de sécurité; (b) déterminer le trafic, les protocoles, les applications de la liste blanche, de la liste noire et autorisées, etc., pour les opérations courantes et spéciales; (c) évaluer le temps nécessaire pour étalonner l'activité du réseau; et (d) préparer les outils et les scripts pour la collecte de données. (2) Faire la collecte des données de trafic du réseau, ce qui consiste à : (a) utiliser des outils automatisés pour la capture de données du réseau, ce qui consiste à : i. lancer et surveiller la capture de paquets de données; ii. dépanner les activités de capture de paquets de données; et iii. valider le résultat pour s'assurer que les résultats prévus sont corrects; et (b) utiliser d'autres moyens pour la collecte des données de réseau requises, ce qui comprend les scripts, les commandes, etc. (3) Analyser les données de la capture de paquets et les données accessoires, ce qui consiste à : (a) identifier les sessions distinctes et l'hôte de la source/destination; (b) créer des statistiques; et (c) résumer les activités/paramètres de base, ce qui comprend : i. les heures de pointe et les heures de fréquentation réduite; et ii. l'utilisation de la bande passante et le volume de trafic par application, protocole, port, etc. (4) Produire des rapports et présenter les statistiques.

OREN 002 – Réagir à un cyberévénement

OCOM	Contenu de l'OCOM (ce que les stagiaires doivent être capables de faire à la fin de l'éducation et de l'instruction connexes)
OCOM 002.01 – Détecter une activité qui représente une menace	(1) Recevoir et analyser les alertes du SDI de différentes sources, conformément aux références C35 et C116, ce qui consiste à : (a) déterminer les paramètres de trafic, conformément aux références C57 et C59; (b) extraire les données de trafic du réseau, conformément aux références C77, C78, C95, C96 et C125; (c) extraire les indicateurs de réseau du SDI, conformément aux références C35 et C116; (d) déterminer la validité des alertes, conformément aux références C76, C99, C105, C106 et C107; et (e) enregistrer les faux positifs, conformément à la référence C115. (2) Analyser le trafic du réseau, conformément aux références C14, C58, C65, C97, C116 et C118, ce qui consiste à : (a) analyser les anomalies dans le trafic du réseau à l'aide des métadonnées, conformément aux références C57 et C125; (b) identifier la cartographie du réseau et les empreintes numériques du système d'exploitation;

OCOM	Contenu de l'OCOM (ce que les stagiaires doivent être capables de faire à la fin de l'éducation et de l'instruction connexes)
	(c) enquêter au sujet des comportements liés au trafic, conformément aux références C78 et C125; (d) analyser les journaux des événements des dispositifs de sécurité du périmètre, conformément aux références C116 et C126; (e) extraire les indicateurs du réseau provenant du trafic, conformément aux références C74, C78, C96 et C125.
OCOM 002.02 — Enquêter sur des cyberévénements	(1) Valider les alertes/comportements anormaux par l'analyse du réseau, ce qui consiste à : (a) recueillir les métadonnées, les données de trafic et les registres, ce qui consiste à : i. déterminer les applications et les systèmes d'exploitation d'un dispositif selon le trafic du réseau, conformément aux références C58, C78, C97, C116, C118 et C125; ii. établir le déroulement des événements, conformément aux références C74, C116 et C125; iii. extraire les indicateurs du réseau provenant du trafic, conformément aux références C74, C78, C96 et C125 et iv. déterminer l'emplacement des ressources physiques du réseau, conformément aux références C125, C127 et C128; (b) Reconstituer les activités malveillantes, ce qui consiste à : i. analyser les activités malveillantes, conformément aux références C74, C78 et C125, ii. recueillir des renseignements sur les activités liées au trafic pour déterminer la source de compromission, conformément aux références C78, C116 et C125; iii. Établir les méthodes de compromission, notamment les voies de commandement et de contrôle et l'exfiltration, conformément aux références C14, C70, C73, C108, C114 et C125; iv. relever les tentatives d'exploitation, conformément à la référence C109; v. extraire la capture des paquets pour l'analyse des protocoles, conformément aux références C78, C114 et C125; (c) fournir les résultats préliminaires aux fins d'analyse supplémentaire, ce qui comprend les indicateurs (adresses IP, noms d'hôtes, ports). (2) Analyser les paquets de données capturés, ce qui consiste à : (a) analyser la capture des paquets de données, conformément aux références C57, C58, C74 et C79; (b) extraire les artefacts, conformément aux références C74, C119 et C125; et (c) rassembler les artefacts, conformément à la référence C74. (3) Analyser un maliciel, conformément aux références C74, C77 et C95, ce qui consiste à : (a) analyser les artefacts, conformément à la référence C120; (b) caractériser le maliciel à l'aide d'outils automatisés, conformément aux références C74, C77, C95 et C121; (c) acheminer les incidents de maliciels aux fins d'analyse supplémentaire.

OCOM	Contenu de l'OCOM (ce que les stagiaires doivent être capables de faire à la fin de l'éducation et de l'instruction connexes)
OCOM 002.03 — Produire des rapports internes	(1) Regrouper des données pertinentes pour produire un rapport technique, ce qui consiste à : (a) déceler ou reconnaître l'événement ou le problème; (b) présenter le déroulement de l'incident, preuves à l'appui; (c) indiquer les conclusions et les résultats pertinents qu'il faut communiquer au superviseur, à l'organisme externe ou au client. (d) formuler des recommandations appropriées pour atténuer ou régler l'événement ou le problème. (2) Rédiger l'ébauche du rapport, notamment les éléments suivants, le cas échéant : (a) toute remarque préliminaire ou tout renseignement général; (b) les observations et résultats (risques et vulnérabilités, conclusions des analyses, faits reliés aux systèmes et au réseau/aux données); (c) les conclusions et constatations tirées des observations; et (d) les mesures d'atténuation recommandées pour améliorer la sécurité ou les mesures de reprise recommandées après l'incident.
OCOM 002.04 — Préserver les preuves scientifiques de cybercriminalité	(1) Créer une copie de travail de l'artefact; (2) Conserver l'artefact d'origine; (3) Décrire en détail la nature de l'artefact; (4) Décrire comment il a été obtenu; (5) Préciser quand il a été recueilli; (6) Consigner qui a traité l'artefact et étayer les mesures prises; et (7) Indiquer où l'artefact est conservé.

OREN 003 - Produire un rapport technique

OCOM	Contenu de l'OCOM (ce que les stagiaires doivent être capables de faire à la fin de l'éducation et de l'instruction connexes)
OCOM 003.01 – Regrouper des données pertinentes pour produire un rapport technique	(1) Déceler ou reconnaître l'événement ou le problème. (2) Présenter le déroulement de l'événement ou du problème, preuves à l'appui . (3) Extraire les détails pertinents contenus dans les notes d'analyse du document. (4) Noter les conclusions et les résultats pertinents qu'il faut communiquer au superviseur, à l'organisme externe ou au client. (5) Formuler des recommandations appropriées pour atténuer ou régler l'événement ou le problème.
OCOM 003.02 — Produire un rapport technique	Rédiger l'ébauche du rapport, notamment les éléments suivants, le cas échéant : (1) Toute remarque préliminaire ou tout renseignement général; (2) Les observations et résultats (risques et vulnérabilités, conclusions des analyses, faits reliés aux systèmes et au réseau ou aux données); (3) Les conclusions et constatations tirées des observations; (4) Les mesures d'atténuation ou de reprise après l'incident recommandées pour améliorer la sécurité; et (5) Toute nouvelle information pertinente relative à l'événement ou au problème qui peut rendre le rapport plus exact.

OCOM	Contenu de l'OCOM (ce que les stagiaires doivent être capables de faire à la fin de l'éducation et de l'instruction connexes)
OCOM 003.03 – Produire un rapport technique pour une distribution orale ou écrite	Produire le rapport pour une distribution orale ou écrite, en tenant compte du public et de l'utilisation d'un langage technique approprié, et qui respecte les principes ci-dessous : (1) clarté (le rapport est explicite, détaillé, exhaustif, intelligible et sans ambiguïté); (2) exactitude (la justesse des détails et des faits du rapport); (3) pertinence (le rapport ne contient pas de mots, d'expressions ou d'idées non pertinents); (4) concision (le rapport est concis, les idées et les faits sont exprimés de façon la plus concise possible, sans nuire à la clarté, à la justesse ou à la pertinence); et (5) rapidité de la publication (le rapport est remis dans le respect des délais imposés).

OREN 004 – Préparer un environnement d'analyse

OCOM	Contenu de l'OCOM (ce que les stagiaires doivent être capables de faire à la fin de l'éducation et de l'instruction connexes)
OCOM 004.01 – Installer le matériel requis	Installer le matériel requis, ce qui comprend : (1) Poste de travail, (2) Disque dur, et (3) Commutateur à prises multiples.
OCOM 004.02 – Configurer les dispositifs de sécurité du réseau physique	Configurer les dispositifs de sécurité du réseau physique, ce qui comprend : (1) Routeurs; (2) Commutateurs; (3) Pare-feu; (4) Dispositifs de surveillance du réseau; (5) SDI et SPI.

OCOM	Contenu de l'OCOM (ce que les stagiaires doivent être capables de faire à la fin de l'éducation et de l'instruction connexes)
OCOM 004.03 – Préparer et mettre sur pied des systèmes d'exploitation virtuels	(1) Installer un serveur virtuel (p. ex., entreprise plus type 1 [ESXI]), conformément à la référence C43, ce qui consiste à : (a) installer un poste de travail virtuel d'utilisateur Windows, conformément aux références C27 et C43; (b) installer diverses images virtuelles de postes de travail, conformément aux références C32 et C43; (c) installer diverses images virtuelles mobiles, conformément à la référence C129; (d) configurer des serveurs Windows, ce qui comprend : i. contrôleur de domaine, conformément aux références C28, C29 et C30, ii. serveur de fichiers et d'imprimantes, conformément aux références C28, C29 et C30, iii. serveur de noms de domaine (DNS), conformément aux références C28, C29, C30, C46 et C47; iv. serveur du protocole Dynamic Host Control (DHCP), conformément aux références C28, C29 et C30; v. serveur Exchange, conformément aux références C28, C29, C30 et C48, vi. serveur Web Microsoft Information Internet Server (IIS), conformément aux références C28, C29 et C30; et vii. serveur MySQL, conformément aux références C28, C29 et C30. (2) Préparer les stratégies de groupe en sécurité, ce qui comprend la configuration, conformément aux références C27, C28, C29 et C30. (3) Installer un poste de travail et un serveur virtuels Linux, ce qui consiste à : (a) installer un serveur Web Linux (Linux Apache MySQL et serveur Web PHP [LAMP]), conformément à la référence C45; (b) installer un pare-feu d'applications Web (mod-security pour Apache); (c) installer un poste de travail Linux, conformément à la référence C31. (4) Installer et configurer des systèmes de réseaux virtuels, ce qui comprend : (a) les routeurs, conformément aux références C23, C26 et C49; (b) les commutateurs, conformément aux références C23, C26 et C49; (c) les dispositifs de surveillance du réseau; (d) le SPI; et (e) les pare-feu, conformément aux références C49 et C56. (5) Gérer les instantanés des images virtuelles, conformément à la référence C43, ce qui consiste à : (a) prendre des instantanés virtuels; (b) revenir à des anciens instantanés; (c) revenir à de nouveaux instantanés; et (d) supprimer des instantanés. (6) Installer un environnement de poste de travail virtuel local (poste de travail Virtual Box ou VMware), ce qui comprend l'installation d'une image de SE virtuelle (format .iso), conformément à la référence C43.

OCOM	Contenu de l'OCOM (ce que les stagiaires doivent être capables de faire à la fin de l'éducation et de l'instruction connexes)
OCOM 004.04 — Configurer un logiciel	(1) Installer des logiciels, ce qui comprend : (a) les logiciels d'utilisateur (Adobe, Office, Wireshark); (b) les interpréteurs de scripts (Python, Ruby); et (c) les outils d'analyse de maliciels (Apatedns, InetSim). (2) Configurer les logiciels (logiciels renifleurs de paquets).
OCOM 004.05 – Faire le dépannage des défaillances matérielles des outils	(1) Remplacer le matériel. (2) Configurer les réseaux physiques.
OCOM 004.06 – Faire le dépannage des défaillances logicielles des outils	(1) Résoudre les défaillances logicielles. (2) Désinstaller et installer des applications. (3) Installer et supprimer des correctifs.
OCOM 004.07 – Installer et maintenir les capteurs du réseau	(1) Installer un dispositif de surveillance réseau en ligne et hors bande, conformément à la référence C130, ce qui consiste à : (a) installer un dispositif de surveillance matériel; et (b) miroiter un port de commutateur (par exemple, Hewlett Packard, Cisco). (2) Confirmer le bon fonctionnement du capteur réseau, ce qui consiste à : (a) vérifier la saisie intégrale des paquets, ce qui comprend la conservation de la saisie intégrale des paquets et l'horaire de roulement des paquets saisis; (b) vérifier la conservation des métadonnées; et (c) vérifier les capteurs et signaler les pannes, ce qui implique notamment d'informer le superviseur des fonctions mises en place. (3) Configurer les règles du capteur réseau, ce qui consiste à : (a) créer une règle; (b) faire l'essai de la fonction de cette règle; (c) recommander le déploiement des règles; (d) télécharger les règles dans les capteurs; (e) confirmer la validité des alertes du capteur par rapport au trafic du réseau; et (f) recommander la désactivation des règles.
OCOM 004.08 — Retirer les logiciels et le matériel nécessaire	(1) Désinstaller les logiciels nécessaires, ce qui consiste à : (a) désinstaller des logiciels avec la fonction « ajouter/supprimer des programmes » de Windows; (b) désinstaller des logiciels à partir de la ligne de commande Linux (« apt-get and yum remove »); et (c) formater le disque dur local (programme KillDisk). (2) Désinstaller le matériel requis (par exemple, commutateur, routeur, dispositif de surveillance, prise USB, disque dur).

OREN 005 – Développer des outils logiciels

OCOM	Contenu de l'OCOM (ce que les stagiaires doivent être capables de faire à la fin de l'éducation et de l'instruction connexes)
OCOM 005.01 — Planifier le développement des outils logiciels	(1) Déterminer les défaillances des logiciels, conformément à la référence C17 (chapitres 1, 2, 5, 6, et 18); (2) Transposer les exigences de sécurité en éléments de conception de l'application, ce qui consiste à : (a) cerner les vulnérabilités des logiciels; (b) définir les implications liées à la sécurité du réseau, conformément à la référence C16 (chapitre 8). (3) Préparer les tableaux de flux de travail, ce qui consiste à : (a) intégrer les mesures de sécurité au cycle de développement des logiciels, conformément à la référence C17 (chapitres 3 à 5); et (b) produire un tableau du flux du travail de programmation, conformément aux références C12, C14 (chapitre 12) et C15 (chapitres 13, 14 et 22).
OCOM 005.02 – Concevoir des outils logiciels	(1) Rédiger les documents relatifs aux logiciels, conformément aux références C15 (chapitres 3 à 5) et C17. (2) Programmer des algorithmes personnalisés, ce qui consiste à : (a) concevoir des algorithmes, ce qui consiste à : i. détecter les défauts de codage de base, notamment appliquer les normes de codage et d'essai, conformément aux références C14 (chapitre 12) et C16 (chapitre 1), ii. appliquer les pratiques exemplaires en matière de sécurité et de programmation, ce qui comprend les scripts de programmation et les programmes, conformément aux références C5, C7, C8, C11, C12 et C15; et (b) appliquer les normes en matière de code et d'essai, ce qui comprend les outils d'essai et la mise à l'essai des programmes, ce qui consiste à : i. procéder au débogage des logiciels et aux essais des unités de conception, conformément aux références C15 (chapitre 6) et C17, ii. corriger les erreurs des programmes en apportant les modifications nécessaires et en vérifiant de nouveau le programme pour en confirmer le bon fonctionnement, conformément aux références C15 et C17.
OCOM 005.03 – Concevoir des outils logiciels	(1) Déterminer les correctifs logiciels appropriés et les documenter, conformément à la référence C41. (2) Modifier les logiciels existants, conformément aux références C14 (chapitres 17 et 18), C41 et C42 (chapitre 54), ce qui consiste à : (a) corriger les erreurs; (b) mettre à jour les interfaces; et (c) améliorer la performance. (3) Effectuer l'analyse des risques si une application subit une modification profonde, conformément aux références C14, C41 et C42 (chapitre 54).

Appendice 3

Liste de références pour la qualification du grade de soldat

Les références des OCOM à l'appendice 2 pour la qualification du grade de soldat sont surlignées en jaune.

Ouvrage de référence	Publication
A	**Documents de référence militaires canadiens**
A1	A-P2-002-NDA/PG-B01 CFSE Network Defence Analyst QS/TP
A2	NDSOD Ch 6 & 7 National Defence Security Orders and Directives (http://intranet.mil.ca/en/health-safety-security/security-policies-ndsod.page)
A3	NDSOD Ch 5,6 and 7 National Defence Security Orders and Directives (http://intranet.mil.ca/en/health-safety-security/security-policies-ndsod.page)
A4	ADM(IM) IT Security Policies and Standards (http://admim-smagi.mil.ca/en/security/policies-standards/index.page)
A5	A-SJ-100-002/AS-001 Information System Security – Operational Security Standard for Information Systems (OSSIS) (http://www.forces.gc.ca/en/about-policies-standards-defence-admin-orders-directives-6000/6003-0.page)
A6	CAF Cyber Operations Primer, February 2014, Chief of Force Development
A7	JDN 2017-02, CAF Joint Doctrine Note - Cyber Operations.
A8	DAOD 6002-2 (http://intranet.mil.ca/en/defence-admin-orders-directives/6000/6002-2.page)
B	**Ouvrages de référence des forces militaires alliées (en anglais seulement)**
B1	TSG 158-0020 Conduct A Military Briefing (Forces aériennes des États-Unis) (http://tsg3.us/tnsg_lib/pldc_school/off_advanced/tnsg_158_0020_conduct_briefing/tnsg_158_0020.pdf) (http://tsg3.us/tnsg_lib/pldc_school/off_advanced/tnsg_158_0020_conduct_briefing/tnsg_158_0020_exam.pdf)
B2	Guide de l'utilisateur du Système de coordination des incidents et de la cyberinformation
C	**Références commerciales (en anglais seulement)**
C1	ISBN 978-1-59327-509-9, The practice of Network Security Monitoring: Understanding Incidence Detection and Response.
C2	ISBN 978-0-471-66186-3, Computer Networking – Internet Protocols in Action
C3	ISBN 978-1587202834, Top-Down Network Design
C4	ISBN 978-1593275679, How Linux Works: What Every Superuser Should Know
C5	ISBN 978-1-59327-192-3, Gray Hat Python - Python Programming for Hackers and Reverse Engineers
C6	ISBN 978-1-118-10679-2, Linux Essentials
C7	ISBN 0070131511, Introduction to Algorithms, Second Edition
C8	ISBN 0470383267, Data Structures and Algorithms in Java
C9	ISBN 0534491324, Computer Science: A structured programming approach using C
C10	ISBN 9780133591620, Modern Operating Systems
C11	ISBN 0132143011, Distributed Systems: Concepts and Design
C12	ISBN 0596007124, Head First Design Patterns
C13	ISBN 9780134101613, Computer Organization and Architecture (9e édition)
C14	ISBN 9780321247445, Introduction to computer security
C15	ISBN : 9781593271190, Code Craft: The Practice of Writing Excellent Code
C16	ISBN : 781593274245, Think Like a Programmer: An Introduction to Creative Problem Solving

Ouvrage de référence	Publication
C17	ISBN : 9780471793717, Software Testing: Testing Across the Entire Software Development Life Cycle
C18	Center for Internet Security (CIS) Top 20 Controls (https://www.cisecurity.org/critical-controls/Library.cfm)
C19	Common Vulnerability Scoring System v3.0 (https://www.first.org/cvss)
C20	Using Wireshark to Create Network-Usage Baselines (https://wiki.wireshark.org/KnownBugs/OutOfMemory?action=AttachFile&do=get&target=Using+Wireshark+to+Create+Network-Usage+Baselines.pdf)
C21	ISBN : 9781259589515, CompTIA A+ Certification All-in-One Exam Guide, Ninth Edition (Exams 220-901 & 220-902)
C22	ISBN : 9780071848220, CompTIA Network+ All-In-One Exam Guide, Sixth Edition (Exam N10-006)
C23	ISBN : 9781119288282, CCNA Routing and Switching Complete Study Guide: Exam 100-105, Exam 200-105, Exam 200-125
C24	ISBN : 9780071841245, Security + Certifications
C25	ISBN : 9781119155034, SSFIPS Security Cisco Networks with Sourcefire intrusion Prevention System Study Guide
C26	ISBN : 9781587144349, CCNP Routing and Switching Portable Command Guide
C27	ISBN : 9781597495615, Microsoft Windows 7 Administrator's Reference: Upgrading, Deploying, Managing, and Securing Windows 7
C28	ISBN : 9780470532867, Mastering Windows Server 2008 R2
C29	ISBN : 9781118289426, Mastering Windows Server 2012 R2
C30	ISBN : 9781785888908, Mastering Windows Server 2016
C31	ISBN : 780072193688, All-In-One Linux+ Certification Exam Guide
C32	ISBN : 9780071668972, MAC OSX System Administration
C33	ISBN : 9780071849272, CISSP Exam study Guide
C34	ISBN : 9781593275099, The practice of Network Security Monitoring: understanding Incident Detection and Response
C35	ISBN : 9781597490993, Snort IDS and IPS Toolkit
C36	ISBN : 9781118987056, The Network Security Test Lab a Step by Step Guide
C37	ISBN : 9781783985982, Kali Linux CTF BluePrints
C38	ISBN : 9781785883491, Building Virtual Pentesting Labs for Advanced Penetration Testing – Second Edition
C39	ISBN : 9780132564717, Network Forensics Tracking Hackers Through Cyberspace
C40	ISBN : 9781593272906 Practical Malware Analysis: The Hands on Guide to Dissecting Malicious Software
C41	Best Practices for Applying Service Packs, Hotfixes and Security Patches par Rick Rosato, responsable technique de compte, Microsoft Corporation (https://msdn.microsoft.com/en-us/library/cc750077.aspx)
C42	ISBN : 9781118127063, Computer Security Handbook, Set, 6th Edition
C43	ISBN : 9781118925157, Mastering VMware vSphere 6
C44	ISBN : 9781508532323, Information Assurance Directorate: Spotting the Adversary with Windows Event Log Monitoring
C45	ISBN : 9781539050261, Modern Web Server Administration using Linux and Wordpress
C46	ISBN: 9784873113906, DNS & BIND : Help for system administrators
C47	ISBN : 9780128033067, DNS Security: Defending the Domain Name System
C48	ISBN : 9781118556832, Mastering Microsoft Exchange Server 2013

Ouvrage de référence	Publication
C49	ISBN : 9781587142727, Implementing Cisco IOS Network Security (IINS 640-554) Foundation Learning Guide (2e édition) (Foundation Learning Guides)
C50	ISBN : 9781587052460, Network Security Technologies and Solutions (CCIE Professional Development Series)
C51	ISBN : 9780470527665, CCNA Voice Study Guide: Examen 640-460
C52	ISBN : 9780470527658, CCNA Wireless Study Guide: IUWNE Exam 640-721
C53	ISBN : 9788126543311, CCNA Data Center: Introducing Cisco Data Center Networking Study Guide, Exam 640-911
C54	Cisco Network-Based Intrusion Detection—Functionalities and Configuration (http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Data_Center/ServerFarmSec_2-1/ServSecDC/8_NIDS.pdf)
C55	Kerberos Golden Ticket Protection Mitigating Pass-the-Ticket on Active Directory (http://cert.europa.eu/static/WhitePapers/UPDATED%20-%20CERT-EU_Security_Whitepaper_2014-007_Kerberos_Golden_Ticket_Protection_v1_4.pdf)
C56	ISBN : 9781587143076, Cisco ASA: All-in-one Next-Generation Firewall, IPS, and VPN Services, 3rd Edition
C57	ISBN : 9781593275099, The practice of Network Security Monitoring: Understanding Incidence Detection and Response
C58	ISDB: 9780471661863, Computer Networking – Internet Protocols in Action
C59	ISBN: 9780735712652, Network Intrusion Detection – Third Edition
C60	ISBN : 9781587202834, Top-Down Network Design
C61	ISBN : 9781449319212, IPv6 Essentials, 3rd Edition – Integrating IPv6 into your IPv4 Network
C62	ISBN : 9781593275679, How Linux Works: What Every Superuser Should Know
C63	ISBN : 9781593271923, Gray Hat Python - Python Programming for Hackers and Reverse Engineers
C64	ISBN : 9780735611313, The Hidden Language of Computer Hardware and Software
C65	ISBN : 9780071497282, CCNA Study Guide 640-802
C66	ISBN : 9780321336316, TCP/IP Illustrated, Volume 1: The Protocols (2e édition)
C67	ISBN : 9781118106792, Linux Essentials ISDN
C68	An Introduction to Attack Patterns as A Software Assurance Knowledge Resource – OMG Software Assurance Workshop 2007 (https://capec.mitre.org/documents/An_Introduction_to_Attack_Patterns_as_a_Software_Assurance_Knowledge_Resource.pdf)
C69	Intrusion Detection Systems: A survey of Taxonomy (https://pdfs.semanticscholar.org/7D28/948bdcb530e2c1deedd8d22dd9b54788a634.pdf)
C70	ISBN : 9780071780285, Hacking Exposed 7: Network Security Secrets and Solutions
C71	DNS Sinkhole whitepaper - SANS Institute InfoSec Reading Room (https://www.sans.org/reading-room/whitepapers/dns/dns-sinkhole-33523)
C72	ISBN : 9780596007911, Snort Cookbook
C73	ISBN : 9780128006047, Targeted Cyber Attacks
C74	Wireshark Network Protocol Analyzer: (http://www.wiresharktraining.com)
C75	Validate the legitimacy of an Alert Network tools, including traceroute, nslookup, dig, whois, ping (http://centralops.net)
C76	Validate the legitimacy of an Alert Analyze IPs with multiple IP blacklists and DNS blacklists (http://ipvoid.com)
C77	Tcpdump/libcap (http://www.tcpdump.org)
C78	Cheat Sheets (Headers, ports, and protocols) (http://packetlife.net/library/cheat-sheets/)
C79	RFC 1700 (Port Numbers) (https://www.ietf.org/rfc/rfc1700.txt)

Ouvrage de référence	Publication
C80	IANA (https://www.iana.org/)
C81	All TCP/UDP ports (http://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers)
C82	CCNA Routing and Switching: Introduction to Networks (https://www.netacad.com)
C83	Autorité responsable des adresses IP (https://www.iana.org/)
C84	Autres jeux d'apprentissage de Cisco (https://learningnetwork.cisco.com/community/learning_center/games)
C85	IP Addressing Guide (http://www.tcpipguide.com/free/t_IPAddressing.htm)
C86	Online Subnet Calculator (http://www.subnet-calculator.com/)
C87	Cisco Subnet Game (https://learningnetwork.cisco.com/docs/DOC-1802)
C88	Cisco IP address and Subnet Introduction (In Depth) (http://www.cisco.com/c/en/us/support/docs/ip/routing-information-protocol-rip/13788-3.html)
C89	IPv6 Primers (https://ipv6.he.net/certification/primer.php) (https://fr.wikipedia.org/wiki/IPv6)
C90	IPv6 Certification (https://ipv6.he.net/certification/)
C91	Regex (https://support.sas.com/rnd/base/datastep/perl_regexp/regexp-tip-sheet.pdf)
C92	Common Attack Pattern Enumeration and Classification (CAPEC) (https://capec.mitre.org/index.html)
C93	The TCP/IP Guide (http://www.tcpipguide.com/free/index.htm)
C94	RFC SourceBook (http://www.networksorcery.com/enp/default.htm)
C95	Ngrep (https://www.freebsd.org/cgi/man.cgi?query=ngrep&sektion=8&manpath=FreeBSD+10.1-RELEASE+and+Ports)
C96	Google search operators (https://support.google.com/websearch/answer/2466433)
C97	Common Vulnerability Database (https://cve.mitre.org/)
C98	Validate the legitimacy of an Alert, Scan websites with multiple reputation engines & blacklists (http://urlvoid.com)
C99	Validate the legitimacy of an Alert, American Registry for Internet Numbers (http://arin.net)
C100	Validate the legitimacy of an Alert, Hurricane Electric Border Gateway Protocol (BGP) Toolkit (http://bgp.he.net)
C101	Validate the legitimacy of an Alert, Robtex Swiss Army Knife Internet Tool (http://www.robtex.com)
C102	Validate the legitimacy of an Alert, Alert Signature Websites, Cisco Intrusion Prevention System Signatures (http://tools.cisco.com/security/center/search.x?search=Signature)
C103	Validate the legitimacy of an Alert, Alert Signature Websites, Emerging Threats Snort Rule Database (http://doc.emergingthreats.net/)
C105	Validate the legitimacy of an Alert, Alert Signature Websites, Snort Rules Website and Rule Lookup (https://snort.org/downloads/#rule-downloads)
C106	Sites Web de signature d'alerte (http://manual-snort-org.s3-website-us-east-1.amazonaws.com/)
C107	nmap (https://nmap.org/)
C108	Norme d'exécution des essais de pénétration – Exploitation (http://www.pentest-standard.org/index.php/Exploitation)
C109	Honeypots (https://www.sans.org/security-resources/idfaq/what-is-a-honeypot/1/9)
C110	Know Your Enemy; Honey Net (http://old.honeynet.org/papers/honeynet).
C111	FAQ sur la détection des intrusions (https://www.sans.org/security-resources/idfaq/are-there-limitations-of-intrusion-signatures/1/21)

Ouvrage de référence	Publication
C112	Guide de règles de Suricata (https://redmine.openinfosecfoundation.org/projects/suricata/wiki/Suricata_Rules)
C113	PCAP-FILTER, page principale (http://www.tcpdump.org/manpages/pcap-filter.7.html)
C114	Strategies to Reduce False Positives and False Negatives in NIDS (http://www.symantec.com/connect/articles/strategies-reduce-false-positives-and-false-negatives-nids)
C115	Base64 (https://www.base64decode.org/)
C116	Arcsight (SIEM) (http://www8.hp.com/us/en/software-solutions/siem-security-information-event-management/)
C117	History of Encryption (SANS) (https://www.sans.org/reading-room/whitepapers/vpns/history-encryption-730)
C118	SANS Glossary of terms (www.sans.org/security-resources/glossary-of-terms)
C119	PCAP man page (http://www.tcpdump.org/manpages/pcap.3pcap.html)
C120	Cuckoo Sandbox Book (https://downloads.cuckoosandbox.org/docs/)
C121	NetWitness Investigator User Guide 9.8 (https://community.rsa.com/docs/DOC-36525)
C122	Sericata User Guide (http://suricata.readthedocs.io/en/latest)
C123	Yara Documentation (http://yara.readthedocs.io/en/v3.4.0/index.html)
C124	Stix Documentation (http://stixproject.github.io/documentation/)
C125	RSA NetWitness (https://sadocs.emc.com/0_en-us)
C126	Sourcefire 3D System (http://www.cisco.com/c/dam/en/us/td/docs/security/sourcefire/3d-system/53/Sourcefire_3D_System_User_Guide_v53.pdf)
C127	IP Address Geolocation (http://www.ipfingerprints.com/)
C128	IP Address Geolocation (http://www.ip-tracker.org/locator/ip-lookup.php)
C129	ISBN 9781516945863, Intermediate Security Testing with Kali Linux 2
C130	Out of Band Network Tap (https://www.ixiacom.com/company/blog/nsa-does-not-want-you know-about-taps-network-security)
C131	ISBN : 0470613033 - Malware Analyst's Cookbook and DVD: Tools and Techniques for Fighting Malicious Code
C132	ISBN : 1118825098 – The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory.
C133	ISBN : 1118787315 – Practical Reverse Engineering
C134	ISBN : 978-1-59327-716-1 – Rootkits and Bootkits: Reversing Modern Malware and Next Generation Threats.
C135	ISBN : 978-1-59327-793-2 – Practical Forensic Imaging: Securing Digital Evidence with Linux Tools
C136	ISBN : 978-1449626365 – The Rootkit Arsenal: Escape and Evasion in the Dark Corners of the System (2e édition)
C137	ISBN 978-0071832380 – Grey Hat Hacking: The Ethical Hacker's Handbook (quatrième édition)
C138	ISBN 978-1491934944 – Intelligence-Driven Incident Response: Outwitting the Adversary
C139	ISBN 978-1500734756 – Blue Team Handbook: Incident Response Edition: A Condensed field guide for the Cyber Security Incident Responder.
C140	ISBN 978-0071798686 – Incident Response & Computer Forensics (3e édition)
C141	ISBN 978-1118026472 – The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws (2e édition)
C142	ISBN 978-8126558766 – The Antivirus Hackers' Handbook
D	**Autres**

Ouvrage de référence	Publication
D1	National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (NCWF), NIST 800-181 (gouvernement des États-Unis) (http://csrc.nist.gov/publications/drafts/800-181/sp800_181_draft.pdf)
D2	ITSG-38 : Conseils en matière de sécurité des TI – Établissement des zones de sécurité dans un réseau – Considérations de conception relatives au positionnement des services dans les zones (CST) (https://cyber.gc.ca/fr/orientation/considerations-de-conception-relatives-au-positionnement-des-services-dans-les-zones)
D3	ITSG-33 : La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie (CST) (https://cyber.gc.ca/fr/orientation/la-gestion-des-risques-lies-la-securite-des-ti-une-methode-axee-sur-le-cycle-de-vie)
D4	Loi sur la preuve au Canada (https://laws-lois.justice.gc.ca/fra/lois/c-5/TexteComplet.html)
D5	DRDC CORA TM 2013-XXX, Military Activities and Cyber Effects (MACE) Taxonomy, décembre 2013 (en anglais) (http://cradpdf.drdc-rddc.gc.ca/PDFS/unc218/p803340_A1b.pdf)
D6	ITSB-120 Guide d'initiation à la sécurité interdomaines (https://cyber.gc.ca/fr/orientation/guide-dinitiation-la-securite-interdomaines-itsb-120)
D7	ITSB-49 Bulletin de sécurité - Enregistreurs de frappe et logiciels espions (https://cyber.gc.ca/fr/orientation/bulletin-de-securite-enregistreurs-de-frappe-et-logiciels-espions-itsb-49)
D8	ITSG-41 Exigences de sécurité liées aux réseaux locaux sans fil (https://cyber.gc.ca/fr/orientation/exigences-de-securite-liees-aux-reseaux-locaux-sans-fil-itsg-41)
D9	ITSB-96 Correction des systèmes d'exploitation et des applications - Bulletin de sécurité des TI à l'intention du gouvernement du Canada (https://cyber.gc.ca/fr/orientation/correction-des-systemes-dexploitation-et-des-applications-bulletin-de-securite-des-ti)
D10	ITSB-100 Reconnaître les courriels malveillants - Conseils à l'intention du gouvernement du Canada (https://www.cse-cst.gc.ca/fr/publication/itsb-100)
D11	ITSB-89 v3 Les 10 mesures de sécurité des TI visant à protéger les réseaux Internet et l'information du gouvernement du Canada (https://cyber.gc.ca/fr/orientation/les-10-mesures-de-securite-des-ti-visant-proteger-les-reseaux-internet-et-linformation)
D12	ITSG-31 Guide sur l'authentification des utilisateurs pour les systèmes TI (https://www.cse-cst.gc.ca/fr/publication/itsg-31)
D13	Loi sur la protection de l'information (R.S.C., 1985, c. O-5) (https://laws-lois.justice.gc.ca/fra/lois/o-5/)
D14	Code criminel (L.R.C., 1985, c. C-46) Article 184 – Interception des communications (http://laws-lois.justice.gc.ca/eng/acts/C-46/page-41.html?txthl=communications+communication+interception+intercepted+intercept#s-184.2)
D15	Code criminel (L.R.C., 1985, c. C-46) Paragraphe 342.1 (1) – Utilisation non autorisée d'ordinateur (https://laws-lois.justice.gc.ca/fra/lois/c-46/page-77.html)
D16	Code criminal (L.R.C., 1985, c. C-46) Alinéa 430(1.1) – Méfait à l'égard de données informatiques (https://laws-lois.justice.gc.ca/fra/lois/c-46/page-91.html)
D17	CSE OPS-1 (document CLASSIFIÉ)
D18	CSE OPS 5-15 (document CLASSIFIÉ)
D19	CSE CSOI 4-1 (document CLASSIFIÉ)
D20	Canadian SIGINT Security Standards (Document CLASSIFIÉ)
D21	IPO du CORFC – Physical Media Analysis - Forensics Taskings (en anglais)

Ouvrage de référence	Publication
D22	IPO Tp de défense des réseaux informatiques du CORFC, Annexe H, Network Defence Report
D23	DIIGI 2 G2 RLD – Tendances en matière de vecteurs, de charges, de comportement et d'effets
D24	Guide de référence des opérations du CORFC
D25	Outil de travail de l'analyste de surveillance du CORFC
D26	Modèle de rapport de surveillance du CORFC
D27	Notes du bref cours sur la sécurité des réseaux (BCSR), exposés 1-5 sur le réseau informatique
D28	Notes de cours du BCSR, exposés 1-5 sur les protocoles Internet
D29	Notes de cours du BCSR, exposé 1 sur l'architecture de sécurité
D30	Notes de cours du BCSR, exposés 1-5 sur les systèmes d'exploitation
D31	Exposé du cours d'OEM OCFC – Jour tech 3 (Reconnaissance, Maintaining Access, Gaining Access)
D32	Exposé du cours d'OEM OCFC 1501 – Network Defence

ANNEXE B, LISTE DE VÉRIFICATION DES EXIGENCES RELATIVES À LA SÉCURITÉ

Government of Canada / Gouvernement du Canada

Contract Number / Numéro du contrat
W4938-21-330S

Security Classification / Classification de sécurité
UNCLASSIFIED

SECURITY REQUIREMENTS CHECK LIST (SRCL)
LISTE DE VÉRIFICATION DES EXIGENCES RELATIVES À LA SÉCURITÉ (LVERS)

PART A - CONTRACT INFORMATION / PARTIE A - INFORMATION CONTRACTUELLE

1. Originating Government Department or Organizati Ministère ou organisme gouvernemental d'origine: DND	2. Branch or Directorate / Direction générale ou Direction: Canadian Defence Academy/DG Cyber
3. a) Subcontract Number / Numéro du contrat de sous-traitance	3. b) Name and Address of Subcontractor / Nom et adresse du sous-traitant

4. Brief Description of Work / Brève description du travail

Service provider to develop and deliver an Assessment tool and courses in support of Cyber Op training program to CAF members identified in the Statement of Work.

5. a) Will the supplier require access to Controlled Goods? Le fournisseur aura-t-il accès à des marchandises contrôlées?	✔ No Non	☐ Yes Oui
5. b) Will the supplier require access to unclassified military technical data subject to the provisions of the Technical Data Control Regulations? Le fournisseur aura-t-il accès à des données techniques militaires non classifiées qui sont assujetties aux dispositions du Règlement sur le contrôle des données techniques?	✔ No Non	☐ Yes Oui
6. Indicate the type of access required / Indiquer le type d'accès requis		
6. a) Will the supplier and its employees require access to PROTECTED and/or CLASSIFIED information or assets? Le fournisseur ainsi que les employés auront-ils accès à des renseignements ou à des biens PROTÉGÉS et/ou CLASSIFIÉS? (Specify the level of access using the chart in Question 7. c) (Préciser le niveau d'accès en utilisant le tableau qui se trouve à la question 7. c)	☐ No Non	✔ Yes Oui
6. b) Will the supplier and its employees (e.g. cleaners, maintenance personnel) require access to restricted access areas? No access to PROTECTED and/or CLASSIFIED information or assets is permitted. Le fournisseur et ses employés (p. ex. nettoyeurs, personnel d'entretien) auront-ils accès à des zones d'accès restreintes? L'accès à des renseignements ou à des biens PROTÉGÉS et/ou CLASSIFIÉS n'est pas autorisé.	✔ No Non	☐ Yes Oui
6. c) Is this a commercial courier or delivery requirement with **no** overnight storage? S'agit-il d'un contrat de messagerie ou de livraison commerciale **sans** entreposage de nuit?	✔ No Non	☐ Yes Oui

7. a) Indicate the type of information that the supplier will be required to access / Indiquer le type d'information auquel le fournisseur devra avoir accès

Canada ✔	**NATO / OTAN** ☐	**Foreign / Étranger** ☐
7. b) Release restrictions / Restrictions relatives à la diffusion		
No release restrictions Aucune restriction relative à la diffusion ✔	All NATO countries Tous les pays de l'OTAN ☐	No release restrictions Aucune restriction relative à la diffusion ☐
Not releasable À ne pas diffuser ☐		
Restricted to: / Limité à : ☐	Restricted to: / Limité à : ☐	Restricted to: / Limité à : ☐
Specify country(ies): / Préciser le(s) pays :	Specify country(ies): / Préciser le(s) pays :	Specify country(ies): / Préciser le(s) pays :
7. c) Level of information / Niveau d'information		
PROTECTED A / PROTÉGÉ A ✔	NATO UNCLASSIFIED / NATO NON CLASSIFIÉ ☐	PROTECTED A / PROTÉGÉ A ☐
PROTECTED B / PROTÉGÉ B ☐	NATO RESTRICTED / NATO DIFFUSION RESTREINTE ☐	PROTECTED B / PROTÉGÉ B ☐
PROTECTED C / PROTÉGÉ C ☐	NATO CONFIDENTIAL / NATO CONFIDENTIEL ☐	PROTECTED C / PROTÉGÉ C ☐
CONFIDENTIAL / CONFIDENTIEL ☐	NATO SECRET / NATO SECRET ☐	CONFIDENTIAL / CONFIDENTIEL ☐
SECRET / SECRET ☐	COSMIC TOP SECRET / COSMIC TRÈS SECRET ☐	SECRET / SECRET ☐
TOP SECRET / TRÈS SECRET ☐		TOP SECRET / TRÈS SECRET ☐
TOP SECRET (SIGINT) / TRÈS SECRET (SIGINT) ☐		TOP SECRET (SIGINT) / TRÈS SECRET (SIGINT) ☐

Government of Canada / Gouvernement du Canada

Contract Number / Numéro du contrat
W4938-21-330S

Security Classification / Classification de sécurité
UNCLASSIFIED

PART A *(continued)* / PARTIE A *(suite)*

8. Will the supplier require access to PROTECTED and/or CLASSIFIED COMSEC information or assets? — ✔ No / Non ☐ Yes / Oui
Le fournisseur aura-t-il accès à des renseignements ou à des biens COMSEC désignés PROTÉGÉS et/ou CLASSIFIÉS?
If Yes, indicate the level of sensitivity:
Dans l'affirmative, indiquer le niveau de sensibilité :

9. Will the supplier require access to extremely sensitive INFOSEC information or assets? — ✔ No / Non ☐ Yes / Oui
Le fournisseur aura-t-il accès à des renseignements ou à des biens INFOSEC de nature extrêmement délicate?

Short Title(s) of material / Titre(s) abrégé(s) du matériel :
Document Number / Numéro du document :

PART B - PERSONNEL (SUPPLIER) / PARTIE B - PERSONNEL (FOURNISSEUR)

10. a) Personnel security screening level required / Niveau de contrôle de la sécurité du personnel requis

✔ RELIABILITY STATUS / COTE DE FIABILITÉ	☐ CONFIDENTIAL / CONFIDENTIEL	☐ SECRET / SECRET	☐ TOP SECRET / TRÈS SECRET
☐ TOP SECRET– SIGINT / TRÈS SECRET – SIGINT	☐ NATO CONFIDENTIAL / NATO CONFIDENTIEL	☐ NATO SECRET / NATO SECRET	☐ COSMIC TOP SECRET / COSMIC TRÈS SECRET
☐ SITE ACCESS / ACCÈS AUX EMPLACEMENTS			

Special comments:
Commentaires spéciaux :

NOTE: If multiple levels of screening are identified, a Security Classification Guide must be provided.
REMARQUE : Si plusieurs niveaux de contrôle de sécurité sont requis, un guide de classification de la sécurité doit être fourni.

10. b) May unscreened personnel be used for portions of the work? — ✔ No / Non ☐ Yes / Oui
Du personnel sans autorisation sécuritaire peut-il se voir confier des parties du travail?
If Yes, will unscreened personnel be escorted? — ☐ No / Non ☐ Yes / Oui
Dans l'affirmative, le personnel en question sera-t-il escorté?

PART C - SAFEGUARDS (SUPPLIER) / PARTIE C - MESURES DE PROTECTION (FOURNISSEUR)

INFORMATION / ASSETS / RENSEIGNEMENTS / BIENS

11. a) Will the supplier be required to receive and store PROTECTED and/or CLASSIFIED information or assets on its site or premises? — ✔ No / Non ☐ Yes / Oui
Le fournisseur sera-t-il tenu de recevoir et d'entreposer sur place des renseignements ou des biens PROTÉGÉS et/ou CLASSIFIÉS?

11. b) Will the supplier be required to safeguard COMSEC information or assets? — ✔ No / Non ☐ Yes / Oui
Le fournisseur sera-t-il tenu de protéger des renseignements ou des biens COMSEC?

PRODUCTION

11. c) Will the production (manufacture, and/or repair and/or modification) of PROTECTED and/or CLASSIFIED material or equipment occur at the supplier's site or premises? — ✔ No / Non ☐ Yes / Oui
Les installations du fournisseur serviront-elles à la production (fabrication et/ou réparation et/ou modification) de matériel PROTÉGÉ et/ou CLASSIFIÉ?

INFORMATION TECHNOLOGY (IT) MEDIA / SUPPORT RELATIF À LA TECHNOLOGIE DE L'INFORMATION (TI)

11. d) Will the supplier be required to use its IT systems to electronically process, produce or store PROTECTED and/or CLASSIFIED information or data? — ✔ No / Non ☐ Yes / Oui
Le fournisseur sera-t-il tenu d'utiliser ses propres systèmes informatiques pour traiter, produire ou stocker électroniquement des renseignements ou des données PROTÉGÉS et/ou CLASSIFIÉS?

11. e) Will there be an electronic link between the supplier's IT systems and the government department or agency? — ✔ No / Non ☐ Yes / Oui
Disposera-t-on d'un lien électronique entre le système informatique du fournisseur et celui du ministère ou de l'agence gouvernementale?

Government of Canada / Gouvernement du Canada

Contract Number / Numéro du contrat
W4938-21-330S

Security Classification / Classification de sécurité
UNCLASSIFIED

PART C - *(continued)* / PARTIE C - *(suite)*

For users completing the form **manually** use the summary chart below to indicate the category(ies) and level(s) of safeguarding required at the supplier's site(s) or premises.
Les utilisateurs qui remplissent le formulaire **manuellement** doivent utiliser le tableau récapitulatif ci-dessous pour indiquer, pour chaque catégorie, les niveaux de sauvegarde requis aux installations du fournisseur.

For users completing the form **online** (via the Internet), the summary chart is automatically populated by your responses to previous questions.
Dans le cas des utilisateurs qui remplissent le formulaire **en ligne** (par Internet), les réponses aux questions précédentes sont automatiquement saisies dans le tableau récapitulatif.

SUMMARY CHART / TABLEAU RÉCAPITULATIF

Category Catégorie	PROTECTED PROTÉGÉ			CLASSIFIED CLASSIFIÉ			NATO				COMSEC					
	A	B	C	CONFIDENTIAL CONFIDENTIEL	SECRET	TOP SECRET TRÈS SECRET	NATO RESTRICTED NATO DIFFUSION RESTREINTE	NATO CONFIDENTIAL NATO CONFIDENTIEL	NATO SECRET	COSMIC TOP SECRET COSMIC TRÈS SECRET	PROTECTED PROTÉGÉ A	B	C	CONFIDENTIAL CONFIDENTIEL	SECRET	TOP SECRET TRES SECRET
Information / Assets Renseignements / Biens																
Production																
IT Media / Support TI																
IT Link / Lien électronique																

12. a) Is the description of the work contained within this SRCL PROTECTED and/or CLASSIFIED?
La description du travail visé par la présente LVERS est-elle de nature PROTÉGÉE et/ou CLASSIFIÉE?

☑ No / Non ☐ Yes / Oui

If Yes, classify this form by annotating the top and bottom in the area entitled "Security Classification".
Dans l'affirmative, classifier le présent formulaire en indiquant le niveau de sécurité dans la case intitulée « Classification de sécurité » au haut et au bas du formulaire.

12. b) Will the documentation attached to this SRCL be PROTECTED and/or CLASSIFIED?
La documentation associée à la présente LVERS sera-t-elle PROTÉGÉE et/ou CLASSIFIÉE?

☑ No / Non ☐ Yes / Oui

If Yes, classify this form by annotating the top and bottom in the area entitled "Security Classification" and indicate with attachments (e.g. SECRET with Attachments).
Dans l'affirmative, classifier le présent formulaire en indiquant le niveau de sécurité dans la case intitulée « Classification de sécurité » au haut et au bas du formulaire et indiquer qu'il y a des pièces jointes (p. ex. SECRET avec des pièces jointes).

ANNEXE C, ENTENTE DE NON-DIVULGATION

Je soussigné(e), _____ , reconnais que, dans le cadre de mon travail à titre d'employé ou de sous-traitant de _____ , je peux avoir le droit d'accès à des renseignements fournis par ou pour le Canada relativement aux travaux, en vertu du contrat portant le numéro de série W4938-21330S/001/ZH, entre Sa Majesté la Reine du chef du Canada, représentée par le ministre des Travaux publics et des Services gouvernementaux et Ministère de la Défense nationale, y compris des renseignements confidentiels ou des renseignements protégés par des droits de propriété intellectuelle appartenant à des tiers, ainsi que ceux qui sont conçus générés ou produits par l'entrepreneur pour l'exécution des travaux. Aux fins de cette entente, les renseignements comprennent, sans s'y limiter, tous les documents, instructions, directives, données, éléments matériels, avis ou autres, reçus verbalement, sous forme imprimée ou électronique ou autre, et considérés ou non comme exclusifs ou de nature délicate, qui sont divulgués à une personne ou dont une personne prend connaissance pendant l'exécution du contrat.

J'accepte de ne pas reproduire, copier, utiliser, divulguer, diffuser ou publier, en tout ou en partie, de quelque manière ou forme que ce soit les renseignements décrits ci-dessus sauf à une personne employée par le Canada qui est autorisée à y avoir accès. Je m'engage à protéger les renseignements et à prendre toutes les mesures nécessaires et appropriées, y compris celles énoncées dans toute instruction écrite ou orale, émise par le Canada, pour prévenir la divulgation ou l'accès à ces renseignements en contravention de cette entente.

Je reconnais également que les renseignements fournis à l'entrepreneur par ou pour le Canada ne doivent être utilisés qu'aux seules fins du contrat et ces renseignements demeurent la propriété du Canada ou d'un tiers, selon le cas.

J'accepte que l'obligation de cette entente survivra à la fin du contrat portant le numéro de série : W4938-21330S/001/ZH.

_____
Signature

_____
Date