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
Formation de cyberopérateurs

Solicitation No. - N° de l'invitation	Date
W4938-20069S/A	2019-12-17

Client Reference No. - N° de référence du client
W4938-20069S

GETS Reference No. - N° de référence de SEAG
PW-$$ZH-113-37169

File No. - N° de dossier	CCC No./N° CCC - FMS No./N° VME
113zh.W4938-20069S	

Solicitation Closes - L'invitation prend fin
at - à 02:00 PM
on - le 2020-01-31

Time Zone
Fuseau horaire
Eastern Standard Time
EST

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	

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

TABLE DES MATIÈRES

TITRE

Demande de soumissions # W4938-20069S/A pour la prestation des services professionnels suivants : programme de formation de 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 attestations et renseignements supplémentaires, et les critères techniques.

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 fournira, à compter d'août 2020, un programme de formation de cyberopérateurs qui répondra aux exigences en matière de rendement de la qualification au grade de soldat cyberopérateur des Forces armées canadiennes. 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 (RCN).

La période du contrat est à partir de la date de signature du contrat jusqu'au 31 décembre 2021 inclusivement avec une option de prolonger la durée du contrat d'au plus quatre périodes supplémentaires de 17-mois chacune.

Ce besoin est assujetti aux dispositions de l'Accord de libre-échange nord-américain (ALENA), de l'Accord économique et commercial global entre le Canada et l'Union européenne (AECG), 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 à la discrétion unique de l'autorité contractante.

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 (TPSGC).

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 (2019-03-04), 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 au Module de réception des soumissions de TPSGC au plus tard à la date, à l'heure et à l'endroit indiqués à la page 1 de la demande de soumissions.

Les soumissions transmises à TPSGC par courrier électronique ne seront pas acceptées.

Remarque : Pour les soumissionnaires qui choisissent de soumettre une soumission en utilisant Connexion postel pour les demandes de propositions qui ferment au Module de réception des soumissions de TPSGC dans la RCN, l'adresse est :

tpsgc.dgareceptiondessoumissions-abbidreceiving.pwgsc@tpsgc-pwgsc.gc.ca

Remarque : Les soumissions ne seront pas acceptées si elles sont envoyées directement à cette adresse de courriel. Cette adresse de courriel doit être utilisée pour ouvrir une conversation Connexion postel, tel qu'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.

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 Demandes de renseignements – en période de soumission

Toutes les demandes de renseignements doivent être présentées par écrit à l'autorité contractante au moins 10 jours civils avant la date de clôture des soumissions. Pour ce qui est des demandes de renseignements reçues après ce délai, il est possible qu'on ne puisse pas y répondre.

Les soumissionnaires devraient citer le plus fidèlement possible le numéro de l'article de la demande de soumissions auquel se rapporte la question et prendre soin d'énoncer chaque question de manière suffisamment détaillée pour que le Canada puisse y répondre avec exactitude. Les demandes de renseignements techniques qui ont un caractère exclusif doivent porter clairement la mention « exclusif » vis-à-vis de chaque article pertinent. Les éléments portant la mention « exclusif » feront l'objet d'une discrétion absolue, sauf dans les cas où le Canada considère que la demande de renseignements n’a pas un caractère exclusif. Dans ce cas, le Canada peut réviser les questions ou peut demander au soumissionnaire de le faire, afin d'en éliminer le caractère exclusif, et permettre la transmission des réponses à tous les soumissionnaires. Le Canada peut ne pas répondre aux demandes de renseignements dont la formulation ne permet pas de les diffuser à tous les soumissionnaires.

2.5 Lois applicable

Tout contrat subséquent sera interprété et régi selon les lois en vigueur la province de l’Ontario, 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 ne seront pas acceptées;

b) La soumission doit être séparée comme suit :

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

c) Si le soumissionnaire choisit de soumettre sa soumission par voie électronique à l'aide du Service Connexion postel fourni par la Société canadienne des postes :

- Le Canada demande que le soumissionnaire prépare sa soumission selon l'article 08, Transmission par télécopieur ou par le service Connexion postel, des Instructions uniformisées 2003. La section 2 de l'article, Connexion postel, comprend des instructions et conditions; et
- Le système Connexion postel a une limite de 1 Go par message individuel affiché et une limite de 20 Go par conversation;

d) Si le soumissionnaire choisit de soumettre sa soumission au Module de réception des soumissions de TPSGC électroniquement en n'utilisant pas le service Connection postel fourni par la Société canadienne des postes, le Canada demande une enveloppe contenant une copie de la soumission sur un CD/DVD. Le soumissionnaire devrait s'assurer que le numéro d'invitation à soumissionner ainsi que le nom et l'adresse du soumissionnaire sont clairement visibles sur l'enveloppe;

e) Le Canada ne demande pas de copies papier de la soumission. Toutefois, si le soumissionnaire choisit de soumettre sa soumission au Module de réception des soumissions de TPSGC en copies papier, le Canada demande :

Section I : quatre copies papier;
Sections II et III : une copie papier des deux sections; et

f) En cas d'incompatibilité entre le libellé des copies de la soumission énumérées dans la liste suivante, c'est le libellé de la copie qui apparaît en premier sur la liste qui l'emporte sur celui de toute autre copie qui figure plus bas sur la liste :

- La copie de la soumission soumise par voie électronique à l'aide du service Connexion postel fourni par la Société canadienne des postes;
- La copie de la soumission soumise au Module de réception des soumissions de TPSGC électroniquement sur un CD/DVD;
- Les copies papier de la soumission soumise au Module de réception des soumissions de TPSGC.

Conformément à la *Politique sur les marchés du Conseil du Trésor* et à la *Loi canadienne sur l'accessibilité*, les ministères et organismes fédéraux doivent tenir compte des critères et des caractéristiques d'accessibilité lorsqu'ils achètent des biens ou des services. Par conséquent, les soumissionnaires sont encouragés à mettre en évidence toutes les caractéristiques et composantes liées à l'accessibilité dans leur proposition pour l'énoncé des travaux dans l'Annexe A. La DAOD 5023-0, Universalité du service, précise que les militaires doivent être en bonne condition physique, aptes au travail et déployables à exécuter les tâches militaires d'ordre général ainsi que les tâches communes liées à la défense et à la sécurité, en plus des tâches de leur groupe professionnel militaire ou de leur description de groupe professionnel militaire.

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.

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

Si le soumissionnaire choisit de soumettre sa soumission en copies papier, le Canada demande que les soumissionnaires suivent les instructions de présentation décrites ci-après pour préparer leur soumission :

a) utiliser du papier de 8,5 po x 11 po (216 mm x 279 mm); et
b) utiliser un système de numérotation correspondant à celui de la demande de soumissions.

En avril 2006, le Canada a approuvé une politique exigeant que les ministères et organismes fédéraux prennent les mesures nécessaires pour incorporer les facteurs environnementaux dans le processus d'approvisionnement Politique d'achats écologiques (http://www.tpsgc-pwgsc.gc.ca/ecologisation-greening/achats-procurement/politique-policy-fra.html).

Pour aider le Canada à atteindre ses objectifs, les soumissionnaires devraient :

1) utiliser du papier de 8,5 po x 11 po (216 mm x 279 mm) contenant des fibres certifiées provenant d'un aménagement forestier durable et contenant au moins 30 % de matières recyclées; et
2) utiliser un format qui respecte l'environnement: impression noir et blanc, recto-verso/à double face, broché ou agrafé, sans reliure Cerlox, reliure à attaches ni reliure à anneaux.

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

1. 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;

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

3. Au moment de préparer leur soumission financière, les soumissionnaires devraient examiner la clause 4.1.2, Évaluation financière, de la Partie 4; et l'article 7.6, Paiement, de la partie 7;

4. Dans leur soumission financière, les soumissionnaires doivent fournir une ventilation de prix relativement à chaque prix de lot ferme proposé et prix unitaire ferme proposé en réponse au barème de prix détaillé à la pièce jointe 1 de la Partie 3.

a) Coût estimatif total des honoraires professionnels

Pour chaque catégorie de main-d'œuvre, les soumissionnaires doivent fournir le coût estimatif total des honoraires professionnels.

b) Coût estimatif des systèmes et équipement de technologie de l'information

Les soumissionnaires doivent identifier tous les systèmes et équipement de technologie de l'information, et ournir pour chacun d'entre eux, le coût estimatif.

c) Coût estimatif des matériaux et fournitures

Les soumissionnaires doivent identifier toutes les catégories de matériaux et fournir pour chacune d'entre elles, le coût estimatif. Les matériaux et fournitures sont des articles qui seront consommés durant la période de tout contrat subséquent.

d) Coût estimatif des sous-traitants

Les soumissionnaires doivent identifier tous les sous-traitants proposés et fournir une ventilation de prix soumise conformément à l'alinéa 4 de cette section de la Partie 3 de la demande de soumissions pour chacun d'entre eux.

e) Coût estimatif des autres frais directs

Les soumissionnaires doivent identifier toutes les catégories d'autres frais directs prévus (par ex. comme les communications interurbaines, les locations, les frais de transcription, etc.) et fournir pour chacune d'entre elles, le coût estimatif.

f) Taxes applicables

La ventilation de prix ne doit pas comprendre les taxes applicables.

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.

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 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. Les soumissionnaires peuvent ajouter des lignes supplémentaires, au besoin.

1. Le soumissionnaire doit proposer un prix de lot ferme pour une classe de 1 à 12 participants.

Période du contrat	Prix de lot ferme
Honoraires professionnels	
Superviseur de contrat	$
Coordonnateur de programme	$
Professeurs qualifiés	$
Formateurs ou assistants	$
Soutien en technologie de l'information (TI)	$
Autre soutien en matière de main-d'œuvre (p. ex., préposés à l'entretien ménager)	$
Systèmes et équipement de TI	
Matériel	$
Logiciel	$
Compte de courriel étudiant pour 1 à 12 participants avec un espace de stockage d'au moins 1 Go, un compte d'espace Web avec un espace de stockage d'au moins 5 Go ainsi qu'un accès à distance au réseau des participants du soumissionnaire	$
Identification des autres systèmes et équipement de TI par le soumissionnaire	$
Matériaux et fournitures	
Identification des matériaux et fournitures par le soumissionnaire	$
Sous-traitants	
Identification des sous-traitants par le soumissionnaire	$
Autres frais directs	
Identification des autres frais directs par le soumissionnaire	$
Total pour chaque classe durant la période du contrat	$

Période optionnelle 1	Prix de lot ferme
Honoraires professionnels	
Superviseur de contrat	$
Coordonnateur de programme	$
Professeurs qualifiés	$
Formateurs ou assistants	$
Soutien en TI	$
Autre soutien en matière de main-d'œuvre (p. ex., préposés à l'entretien ménager)	$
Systèmes et équipement de TI	
Matériel	$
Logiciel	$
Compte de courriel étudiant pour 1 à 12 participants avec d'un espace de stockage d'au moins 1 Go, un compte d'espace Web avec un espace de stockage d'au moins 5 Go ainsi qu'un accès à distance au réseau des participants du soumissionnaire	$
Identification des autres systèmes et équipement de TI par le soumissionnaire	$
Matériaux et fournitures	
Identification des matériaux et fournitures par le soumissionnaire	$
Sous-traitants	
Identification des sous-traitants par le soumissionnaire	$
Autres frais directs	
Identification des autres frais directs par le soumissionnaire	$
Total pour chaque classe durant la période optionnelle 1	$

Période optionnelle 2	Prix de lot ferme
Honoraires professionnels	
Superviseur de contrat	$
Coordonnateur de programme	$
Professeurs qualifiés	$
Formateurs ou assistants	$
Soutien en TI	$
Autre soutien en matière de main-d'œuvre (p. ex., préposés à l'entretien ménager)	$
Systèmes et équipement de TI	
Matériel	$
Logiciel	$
Compte de courriel étudiant pour 1 à 12 participants avec d'un espace de stockage d'au moins 1 Go, un compte d'espace Web avec un espace de stockage d'au moins 5 Go ainsi qu'un accès à distance au réseau des participants du soumissionnaire	$
Identification des autres systèmes et équipement de TI par le soumissionnaire	$
Matériaux et fournitures	
Identification des matériaux et fournitures par le soumissionnaire	$
Sous-traitants	
Identification des sous-traitants par le soumissionnaire	$
Autres frais directs	
Identification des autres frais directs par le soumissionnaire	$
Total pour chaque classe durant la période optionnelle 2	$

Période optionnelle 3	Prix de lot ferme
Honoraires professionnels	
Superviseur de contrat	$
Coordonnateur de programme	$
Professeurs qualifiés	$
Formateurs ou assistants	$
Soutien en TI	$
Autre soutien en matière de main-d'œuvre (p. ex., préposés à l'entretien ménager)	$
Systèmes et équipement de TI	
Matériel	$
Logiciel	$
Compte de courriel étudiant pour 1 à 12 participants avec d'un espace de stockage d'au moins 1 Go, un compte d'espace Web avec un espace de stockage d'au moins 5 Go ainsi qu'un accès à distance au réseau des participants du soumissionnaire	$
Identification des autres systèmes et équipement de TI par le soumissionnaire	$
Matériaux et fournitures	
Identification des matériaux et fournitures par le soumissionnaire	$
Sous-traitants	
Identification des sous-traitants par le soumissionnaire	$
Autres frais directs	
LIdentification des autres frais directs par le soumissionnaire	$
Total pour chaque classe durant la période optionnelle 3	$

Période optionnelle 4	Prix de lot ferme
Honoraires professionnels	
Superviseur de contrat	$
Coordonnateur de programme	$
Professeurs qualifiés	$
Formateurs ou assistants	$
Soutien en TI	$
Autre soutien en matière de main-d'œuvre (p. ex., préposés à l'entretien ménager)	$
Systèmes et équipement de TI	
Matériel	$
Logiciel	$
Compte de courriel étudiant pour 1 à 12 participants avec d'un espace de stockage d'au moins 1 Go, un compte d'espace Web avec un espace de stockage d'au moins 5 Go ainsi qu'un accès à distance au réseau des participants du soumissionnaire	$
Identification des autres systèmes et équipement de TI par le soumissionnaire	$
Matériaux et fournitures	
Identification des matériaux et fournitures par le soumissionnaire	$
Sous-traitants	
Identification des sous-traitants par le soumissionnaire	$
Autres frais directs	
Identification des autres frais directs par le soumissionnaire	$
Total pour chaque classe durant la période optionnelle 4	$

Tableau 1		Prix de lot ferme (en $ CAN)
		A
1	Période du contrat	$
2	Période optionnelle 1	$
3	Période optionnelle 2	$
4	Période optionnelle 3	$
5	Période optionnelle 4	$
	Total (A1+A2+A3+A4+A5)	$

2. Le soumissionnaire doit proposer un prix unitaire ferme par semestre pour chaque participant additionnel jusqu'à un maximum de 24 participants par classe.

Période du contrat	Prix unitaire ferme
Honoraires professionnels	
Superviseur de contrat	$
Coordonnateur de programme	$
Professeurs qualifiés	$
Formateurs ou assistants	$
Soutien en TI	$
Autre soutien en matière de main-d'œuvre (p. ex., préposés à l'entretien ménager)	$
Systèmes et équipement de TI	
Matériel	$
Logiciel	$
Courriel individuels pour les participants dotés d'un espace de stockage d'au moins 1 Go, un compte d'espace Web avec un espace de stockage d'au moins 5 Go ainsi qu'un accès à distance au réseau des participants du soumissionnaire	$
Identification des autres systèmes et équipement de TI par le soumissionnaire	$
Matériaux et fournitures	
Identification des matériaux et fournitures par le soumissionnaire	$
Sous-traitants	
Identification des sous-traitants par le soumissionnaire	$
Autres frais directs	
Identification des autres frais directs par le soumissionnaire	$
Total pour chaque semestre durant la période du contrat	$

Période optionnelle 1	Prix unitaire ferme
Honoraires professionnels	
Superviseur de contrat	$
Coordonnateur de programme	$
Professeurs qualifiés	$
Formateurs ou assistants	$
Soutien en TI	$
Autre soutien en matière de main-d'œuvre (p. ex., préposés à l'entretien ménager)	$
Systèmes et équipement de TI	
Matériel	$
Logiciel	$
Courriel individuels pour les participants dotés d'un espace de stockage d'au moins 1 Go, un compte d'espace Web avec un espace de stockage d'au moins 5 Go ainsi qu'un accès à distance au réseau des participants du soumissionnaire	$
Identification des autres systèmes et équipement de TI par le soumissionnaire	$
Matériaux et fournitures	
Identification des matériaux et fournitures par le soumissionnaire	$
Sous-traitants	
Identification des sous-traitants par le soumissionnaire	$
Autres frais directs	
Identification des autres frais directs par le soumissionnaire	$
Total pour chaque semestre durant la période optionnelle 1	$

Période optionnelle 2	Prix unitaire ferme
Honoraires professionnels	
Superviseur de contrat	$
Coordonnateur de programme	$
Professeurs qualifiés	$
Formateurs ou assistants	$
Soutien en TI	$
Autre soutien en matière de main-d'œuvre (p. ex., préposés à l'entretien ménager)	$
Systèmes et équipement de TI	
Matériel	$
Logiciel	$
Courriel individuels pour les participants dotés d'un espace de stockage d'au moins 1 Go, un compte d'espace Web avec un espace de stockage d'au moins 5 Go ainsi qu'un accès à distance au réseau des participants du soumissionnaire	$
Identification des autres systèmes et équipement de TI par le soumissionnaire	$
Matériaux et fournitures	
Identification des matériaux et fournitures par le soumissionnaire	$
Sous-traitants	
Identification des sous-traitants par le soumissionnaire	$
Autres frais directs	
Identification des autres frais directs par le soumissionnaire	$
Total pour chaque semestre durant la période optionnelle 2	$

Période optionnelle 3	Prix unitaire ferme
Honoraires professionnels	
Superviseur de contrat	$
Coordonnateur de programme	$
Professeurs qualifiés	$
Formateurs ou assistants	$
Soutien en TI	$
Autre soutien en matière de main-d'œuvre (p. ex., préposés à l'entretien ménager)	$
Systèmes et équipement de TI	
Matériel	$
Logiciel	$
Courriel individuels pour les participants dotés d'un espace de stockage d'au moins 1 Go, un compte d'espace Web avec un espace de stockage d'au moins 5 Go ainsi qu'un accès à distance au réseau des participants du soumissionnaire	$
Identification des autres systèmes et équipement de TI par le soumissionnaire	$
Matériaux et fournitures	
Identification des matériaux et fournitures par le soumissionnaire	$
Sous-traitants	
Identification des sous-traitants par le soumissionnaire	$
Autres frais directs	
Identification des autres frais directs par le soumissionnaire	$
Total pour chaque semestre durant la période optionnelle 3	$

Période optionnelle 4	Prix unitaire ferme
Honoraires professionnels	
Superviseur de contrat	$
Coordonnateur de programme	$
Professeurs qualifiés	$
Formateurs ou assistants	$
Soutien en TI	$
Autre soutien en matière de main-d'œuvre (p. ex., préposés à l'entretien ménager)	$
Systèmes et équipement de TI	
Matériel	$
Logiciel	$
Courriel individuels pour les participants dotés d'un espace de stockage d'au moins 1 Go, un compte d'espace Web avec un espace de stockage d'au moins 5 Go ainsi qu'un accès à distance au réseau des participants du soumissionnaire	$
Identification des autres systèmes et équipement de TI par le soumissionnaire	$
Matériaux et fournitures	
Identification des matériaux et fournitures par le soumissionnaire	$
Sous-traitants	
Identification des sous-traitants par le soumissionnaire	$
Autres frais directs	
Identification des autres frais directs par le soumissionnaire	$
Total pour chaque semestre durant la période optionnelle 4	$

Tableau 2		Prix unitaire ferme par participant par semestre (en $ CAN)	Nombre de semestres	Nombre estimatif de participants additionnels	Sous-total (en $ CAN)
		A	B	C	D = A x B x C
1	Période du contrat	$	4	12	$
2	Période optionnelle 1	$	4	12	$
3	Période optionnelle 2	$	4	12	$
4	Période optionnelle 3	$	4	12	$
5	Période optionnelle 4	$	4	12	$
				Total (D1+D2+D3+D4+D5)	$

3. En ce qui concerne les manuels neufs ou de rechange, le soumissionnaire sera remboursé au prix coûtant, plus les frais administratifs. . Le soumissionnaire doit proposer les frais administratifs. Le coût estimatif de manuels pour chaque période dans le tableau 3 est pour fins d'évaluation financière seulement.

Tableau 3		Frais administratifs	Coût estimatif de manuels	Sous-total (en $ CAN)
		A	B	C = (A x B) + B
1	Période du contrat	%	24 000,00$	$
2	Période optionnelle 1	%	24 000,00$	$
3	Période optionnelle 2	%	24 000,00$	$
4	Période optionnelle 3	%	24 000,00$	$
5	Période optionnelle 4	%	24 000,00$	$
			Total (C1+C2+C3+C4+C5)	$

Sommaire		A (en $ CAN)
1	Total de tableau 1	$
2	Total de tableau 2	$
3	Total de tableau 3	$
	Prix total évalué (Taxes applicables en sus) (A1+A2+A3)	$

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 Évaluation technique

4.1.1.1 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.

4.1.1.2 Critères techniques obligatoires

Voir la pièce jointe 1 de la Partie 4.

4.1.1.3 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.

4.1.2 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

1.1 Critères techniques obligatoires

a) La soumission doit satisfaire aux critères techniques obligatoires qui sont précisés au tableau ci-dessous. Le soumissionnaire doit fournir la documentation nécessaire à l'appui de la conformité.

b) Toute soumission qui ne respecte pas les critères techniques obligatoires sera jugée irrecevable. Chaque critère technique obligatoire devrait être traité séparément.

c) Dans le cas d'une coentreprise, au moins un des membres de la coentreprise doit satisfaire aux critères techniques obligatoires. Le soumissionnaire doit indiquer quel membre de la coentreprise il utilise pour chaque critère technique obligatoire.

d) Dans le cas d'une coentreprise, l'expérience combinée des parties qui forment la coentreprise ne sera pas considérée afin de satisfaire les critères techniques obligatoires.

Numéro	Critères techniques obligatoires (TO)	Instructions aux soumissionnaires
TO1	Le soumissionnaire doit avoir exercé ses activités depuis au moins trois ans précédant la date de publication de la demande de soumissions.	Le soumissionnaire doit fournir : Une copie du certificat d'enregistrement du nom commercial. OU Une copie du certificat d'enregistrement provincial ou territorial de la société par actions. OU Une copie du certificat d'enregistrement fédéral de l'incorporation de l'entreprise.
TO2	Le soumissionnaire doit avoir un centre de formation et des installations situés dans les limites géographiques de Kingston (Ontario) ou dans la région de la capitale nationale.	Le soumissionnaire doit fournir l'adresse complète du centre de formation et des installations (adresse municipale, municipalité ou ville, province et code postal).

Numéro	Critères techniques obligatoires (TO)	Instructions aux soumissionnaires
TO3	Le centre de formation et les installations du soumissionnaire doivent comprendre une salle de classe ou un laboratoire informatique qui respecte les exigences suivantes : a) Pouvoir accueillir jusqu'à 24 participants; b) Être équipé de bureaux et de chaises pour accueillir jusqu'à 24 participants; c) Être équipé d'au moins 24 ordinateurs de bureau ou portatifs, qui doivent tous comprendre : i. Une connexion et un accès à Internet; ii. Les logiciels indiqués à la section 9.11 de l'énoncé des travaux; d) Être doté des périphériques destinés aux opérations cybernétiques, en plus d'être doté d'une configuration pour le réseau de soutien à l'information; e) Posséder une infrastructure de serveur et de réseau à l'appui des objectifs de formation; et f) Avoir un photocopieur.	Le soumissionnaire doit fournir une description détaillée de la salle de classe ou du laboratoire informatique pour démontrer qu'il satisfait aux exigences.
TO4	Le centre de formation et les installations du soumissionnaire doivent comprendre un espace de bureau doté : a) De deux salles pour une personne, comprenant un bureau, une chaise, un téléphone individuel et un accès à une ligne de communication de données (p. ex. Internet, réseau local); et b) D'une salle privée comprenant un bureau et deux chaises.	Le soumissionnaire doit fournir une description détaillée de l'espace de bureau pour démontrer qu'il satisfait aux exigences.
TO5	Le centre de formation et les installations du soumissionnaire doivent comprendre une aire de repas qui respecte les exigences suivantes : a) Être distincte de la salle de classe ou du laboratoire informatique; b) Pouvoir accueillir les 24 participants de sorte qu'ils soient en mesure de prendre leur repas en groupe; c) Comprendre un réfrigérateur; et d) Comprendre un four à micro-ondes.	Le soumissionnaire doit fournir une description détaillée de l'aire de repas pour démontrer qu'elle satisfait aux exigences.

Numéro	Critères techniques obligatoires (TO)	Instructions aux soumissionnaires
TO6	Le programme de formation de cyberopérateur du soumissionnaire doit être reconnu par une autorité éducative canadienne reconnue par la province.	Le soumissionnaire doit fournir : a) Des documents juridiques (p. ex., certificat d'accréditation, mandat); b) Des politiques d'évaluation des participants, des procédures de notation et des grilles d'évaluation; c) Des politiques et procédures concernant l'aide à l'appentissage (une ébauche est acceptable); d) Les lignes directrices et règlements transmis aux participants, y compris la politique relative au changement de cours; et e) Une copie vierge et non signée du diplôme qui serait remis aux participants qui terminent le programme.
TO7	Le soumissionnaire doit fournir un plan de ressources humaines portant sur le recrutement et le remplacement de ressources qualifiées pouvant offrir les services indiqués dans l'énoncé des travaux.	Le soumissionnaire doit fournir : a) Le processus d'évaluation et de sélection des enseignants et des formateurs ainsi que des assistants qualifiés; b) La stratégie et le processus utilisés pour respecter le ratio d'élèves par professeur et assistant, qui est de 12:1; et c) La stratégie et le processus utilisés pour remplacer les ressources qualifiées en temps opportun, de façon à 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) Le soumissionnaire doit fournir le nom de tous les individus qui devront avoir accès à des renseignements ou à des biens de nature protégée ou classifiée ou à des établissements de travail dont l'accès est réglementé.

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 Travaux publics et Services gouvernementaux Canada (https://www.tpsgc-pwgsc.gc.ca/esc-src/introduction-fra.html).

PARTIE 7 – CLAUSES DU CONTRAT SUBSÉQUENT

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

7.1 Énoncé des travaux

L'entrepreneur doit exécuter les travaux conformément à l'énoncé des travaux, 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 (2018-06-21), Conditions générales - besoins plus complexes de services, s'appliquent au contrat et en font partie intégrante.

La section 20 de 2035 Conditions générales - besoins plus complexes de services, est supprimée en totalité.

7.2.2 Conditions générales supplémentaires

4006 (2010-08-16), L'entrepreneur 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 l'autorité technique avant de leur donner accès aux renseignements fournis par ou pour le Canada relativement aux travaux.

7.3 Exigences relatives à la sécurité

7.3.1 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 :

a) 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 du Secteur de la sécurité industrielle (SSI) de TPSGC;

b) Les membres du personnel de l'entrepreneur devant avoir accès à des renseignements ou à des biens PROTÉGÉS, ou à des établissements de travail dont l'accès est réglementé, doivent TOUS détenir une cote de FIABILITÉ en vigueur, délivrée ou approuvée par le PSC/SSI/TPSGC;

c) L'entrepreneur NE DOIT PAS emporter de renseignements ou de biens PROTÉGÉS hors des établissements de travail visés; et l'entrepreneur doit s'assurer que son personnel est au courant de cette restriction et qu'il la respecte;

d) Les contrats de sous-traitance comportant des exigences relatives à la sécurité NE DOIVENT PAS être attribués sans l'autorisation écrite préalable du PSC/SSI/TPSGC; et

e) L'entrepreneur ou l'offrant doit respecter les dispositions :

i. de la Liste de vérification des exigences relatives à la sécurité et directive de sécurité (s'il y a lieu), reproduite ci-joint à l'Annexe B;
ii. du *Manuel de la sécurité industrielle* (dernière édition).

7.4 Durée du contrat

7.4.1 Période du contrat

La période du contrat est à partir de la date du contrat jusqu'au 31 décembre 2021 inclusivement.

7.4.2 Option de prolongation du contrat

L'entrepreneur accorde au Canada l'option irrévocable de prolonger la durée du contrat pour au plus quatre période(s) supplémentaire(s) de 17-mois chacune, selon les mêmes conditions. L'entrepreneur accepte que pendant la période prolongée du contrat, il sera payé conformément aux dispositions applicables prévues à la Base de paiement.

Le Canada peut exercer cette option à n'importe quel moment, en envoyant un avis écrit à l'entrepreneur au moins 90 jours civils avant la date d'expiration du contrat. Cette option ne pourra être exercée que par l'autorité contractante et sera confirmée, pour des raisons administratives seulement, par une modification au contrat.

7.4.3 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 Responsables

7.5.1 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.

7.5.2 Responsable technique

L'authorité technique pour le contrat est :

À insérer au moment de l'attribution du contrat

L'authorité 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 l'authorité 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.

7.5.3 Représentant de l'entrepreneur

À insérer au moment de l'attribution du contrat

7.6 Paiement

7.6.1 Base de paiement

7.6.1.1 Prix de lot ferme

a) Pour les travaux décrits dans l´Énoncé des travaux à l´annexe A à l'exception des participants additionnels ou des manuels neufs ou de rechange, l'entrepreneur sera payé un prix de lot ferme figurant ci-dessous pour une classe de 1 à 12 participants. Le prix de lot ferme comprend tous les coûts associés à la prestation de la formation, les droits de douane sont inclus et les taxes applicables sont en sus.

Période du contrat	Période optionnelle 1	Période optionnelle 2	Période optionnelle 3	Période optionnelle 4
À insérer au moment de l'attribution du contrat $	*À insérer au moment de l'attribution du contrat* $	*À insérer au moment de l'attribution du contrat* $	*À insérer au moment de l'attribution du contrat* $	*À insérer au moment de l'attribution du contrat* $

b) 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.

7.6.1.2 Prix unitaire ferme

a) L'entrepreneur sera payé un prix unitaire ferme par stagiaire par semestre figurant ci-dessous pour chaque stagiaire additionnel jusqu'à un maximum de 24 participants par classe. Le prix unitaire ferme par participant par semestre comprend tous les coûts associés à la prestation de la formation pour chaque semestre pour chaque stagiaire additionnel, les droits de douane sont inclus et les taxes applicables sont en sus.

Période du contrat	Période optionnelle 1	Période optionnelle 2	Période optionnelle 3	Période optionnelle 4
À insérer au moment de l'attribution du contrat $	*À insérer au moment de l'attribution du contrat* $	*À insérer au moment de l'attribution du contrat* $	*À insérer au moment de l'attribution du contrat* $	*À insérer au moment de l'attribution du contrat* $

b) 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.

7.6.1.3 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* %

7.6.2 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.

7.6.3 Méthode de paiemen

7.6.3.1 Paiements d'étape

a) Pour les travaux décrits dans l'Énoncé des travaux à l'annexe A à l'exception des participants additionnels ou des manuels neufs ou de rechange, le Canada effectuera les paiements d'étape conformément au calendrier des étapes détaillé dans le contrat et les dispositions de paiement du contrat si :
   i. une demande de paiement exacte et complète en utilisant le formulaire PWGSC-TPSGC 1111, Demande de paiement progressif (https://www.tpsgc-pwgsc.gc.ca/app-acq/forms/1111-fra.html), et tout autre document exigé par le contrat ont été présentés conformément aux instructions relatives à la facturation fournies dans le contrat;
   ii. toutes les attestations demandées sur le formulaire PWGSC-TPSGC 1111 ont été signées par les représentants autorisés; et
   iii. tous les travaux associés à l'étape et, selon le cas, tout bien livrable exigé ont été complétés et acceptés par le Canada;

b) Le calendrier des étapes selon lequel les paiements seront faits en vertu du contrat est comme suit :

Numéro de l'étape	Description	Montant ferme
1	À la fin du premier semestre	40% du prix de lot ferme
2	À la fin du deuxième semestre	20% du prix de lot ferme
3	À la fin du troisième semestre	20% du prix de lot ferme
4	À la fin du quatrième semestre	20% du prix de lot ferme

7.6.3.2 Paiement unique

a) Pour chaque stagiaire additionnel, le Canada paiera l'entrepreneur à la fin de chaque semestre 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;

b) 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.

7.6.3 Clauses du guide des CCUA

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

7.6.4 Vérification discrétionnaire

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

7.6.6 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 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) Les factures doivent être distribuées comme suit :

i. 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

ii. 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.

7.8 Attestations et renseignements supplémentaires

7.8.1 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.

7.8.2 Programme de contrats fédéraux pour l'équité en matière d'emploi - Manquement de la part de l'entrepreneur

Lorsqu'un Accord pour la mise en oeuvre de l'équité en matière d'emploi a été conclu avec Emploi et Développement social Canada (EDSC) - Travail, l'entrepreneur reconnaît et s'engage, à ce que cet accord demeure valide pendant toute la durée du contrat. Si l'Accord pour la mise en oeuvre de l'équité en matière d'emploi devient invalide, le nom de l'entrepreneur sera ajouté à la « Liste des soumissionnaires à admissibilité limitée du PCF » du Programme de contrats fédéraux (PCF) pour l'équité en matière d'emploi disponible au bas de la page du site Web d'Emploi et Développement social Canada (EDSC) – Travail (https://www.canada.ca/fr/emploi-developpement-social/programmes/equite-emploi/programme-contrats-federaux.html). L'imposition d'une telle sanction par EDSC fera en sorte que l'entrepreneur sera considéré non conforme aux modalités du contrat.

7.9 Lois applicables

Le contrat doit être interprété et régi selon les lois en vigueur la province de l'Ontario, Canada et les relations entre les parties seront déterminées par ces lois.

7.10 Ordre de priorité des documents

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

a) les articles de la convention;
b) les conditions générales supplémentaires 4006 (2010-08-16), L'entrepreneur détient les droits de propriété intellectuelle sur les renseignements originaux;
c) les conditions générales 2035 (2018-06-21), Conditions générales - besoins plus complexes de services;
d) l'Annexe A, l'énoncé des travaux;
e) l'Annexe B, la LVERS;
f) l'Annexe C, l'entente de non-divulgation; et
g) la soumission de l'entrepreneur datée du *À insérer au moment de l'attribution du contrat.*

7.11 Contrat de défense

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

7.12 Ressortissants étrangers

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

7.13 Assurance

G1005C (2016-01-28), Assurances

7.14 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).

ANNEXE A

ÉNONCÉ DES TRAVAUX

1. TITRE

Formation des cyberopérateurs

2. OBJECTIF

Le présent énoncé des travaux vise à obtenir les services d'un entrepreneur qui fournira, à compter d'août 2020, un programme de formationqui satisfera aux exigences en matière de rendement de la qualification au grade de soldat (QG de sdt) cyberopérateur des Forces armées canadiennes (FAC).

3. CONTEXTE

3.1 En 2010, le Vice-Chef d'état-major de la défense a confié à la force opérationnelle cybernétique le mandat d'institutionnaliser et de mettre en place rapidement une nouvelle capacité cybernétique pour les FAC. Ce mandat a par la suite été confié au Directeur - Développement de la force cybernétique. Le besoin de former un effectif institutionnalisé, spécialisé et dévoué pour la conduite de cyberopérations, qui a été appuyé par la politique de défense du Canada - Protection, Sécurité, Engagement en juin 2017, fait partie intégrante de ce mandat. En outre, cette politique de défense a fourni au ministère de la Défense nationale (MDN) et aux FAC un large éventail d'initiatives qui continueront de faire croître les capacités de combat du Canada, y compris plusieurs capacités directement liées à la lutte cybernétique telles que l'amélioration de la force cybernétique des FAC réalisée au moyen de la création d'un nouveau poste de cyberopérateur. Ce nouveau poste a été créé et approuvé en 2017.

3.2 Les cyberopérateurs sont membres de la Branche de l'électronique et des communications des FAC. Ils réalisent des opérations cybernétiques de défense et, selon le besoin et la faisabilité, des opérations cybernétiques actives. De plus, ils communiquent et collaborent avec des ministères et des organismes gouvernementaux ainsi qu'avec des alliés du Canada, en vue d'accroître la capacité du MDN et des FAC d'offrir un environnement cybernétique sécurisé. Ils surveillent les réseaux de communication des FAC afin de déceler toute tentative d'accès non autorisé au réseau et d'intervenir, le cas échéant. En outre, ils fournissent un soutien cybernétique afin de combler les besoins opérationnels de la Marine, de l'Armée, de l'Aviation et des éléments habilitants interarmées. Les cyberopérateur assument les responsabilités suivantes :

a. recueillir, traiter et analyser des données réseau;
b. relever les vulnérabilités réseau;
c. gérer un environnement de réseaux informatiques;
d. mener des cyberopérations défensives et actives;
e. mettre à profit ses connaissances en matière de sécurité et de communication dans le domaine de la technologie de l'information (TI); et
f. utiliser et tenir à jour des publications ainsi que des dossiers classifiés et non classifiés.

3.3 Un principe directeur qui découle de l'élaboration de ce nouveau poste est le fait que les spécialistes des cyberopérations requièrent de la formation et une éducation considérables pour être efficaces. Une importante partie de cette formation et de cette éducation est identique à celle que doivent suivre les spécialistes des cyberopérations civils, alors que certains autres aspects sont propres aux réseaux et systèmes du MDN et des FAC. Les difficultés relatives à la prestation de la formation et de l'éducation dont les cyberopérateurs ont besoin, indiquées ci-dessous, ont été soulignées au cours des études initiales et persistent toujours.

a. Il n'existe pas de formation et d'éducation propres au poste de cyberopérateur au sein des FAC;
b. À l'heure actuelle, les FAC ne sont dotées d'aucun groupe de formateurs à temps plein qui possèdent le niveau d'éducation, de formation et d'expérience spécifique aux FAC requis pour préparer, offrir et maintenir un programme complet de formation et d'éducation à l'intention des cyberopérateurs de premier échelon; et
c. Les exigences en matière d'infrastructure associées à l'exécution de tous les volets du nouveau programme de formation des cyberopérateurs dépassent la capacité de l'École d'électronique et de communications des Forces canadiennes (EECFC).

3.4 Au sein des FAC, l'instruction des cyberopérateurs a été assignée aux organisations suivantes :

a. L'EECFC est responsable de l'instruction des participants et de leur gestion individuelle. L'authorité technique peut désigner une unité autre que l'EECFC à sa discrétion et avisera l'entrepreneur par courriel;
b. Le Groupe de l'instruction de la Génération du personnel militaire (GIGPM) est responsable de la gestion et de l'administration des programmes de formation. L'authorité technique peut désigner une unité autre que le GIGPM à sa discrétion et avisera l'entrepreneur par courriel; et
c. Le directeur général du développement de la Force cybernétique (DG DF Cyber) est l'authorité technique et constitue la principale personne-ressource pour l'entrepreneur. Il lui incombe de conseiller l'EECFC et le GIGPM en ce qui concerne toutes les tâches et toutes les questions techniques relatives au poste de cyberopérateur.

3.5 La norme de qualification et plan (NQP) relative à la QG de sdt cyberopérateur en 2017 a été élaboré, avec les difficultés énoncées à la section 3.3. Les objectifs de rendement (OREN) compris dans cette NQP décrivent les tâches que le participant doit être en mesure d'accomplir pour obtenir la QG de sdt, notamment :

a. OREN 001 – Maintenir une connaissance de la situation du réseau;
b. OREN 002 – Réagir à un cyberévénement;
c. OREN 003 – Produire un rapport technique;
d. OREN 004 – Préparer un environnement d'analyse;
e. OREN 005 – Développer des outils logiciels;
f. OREN 006 – Appliquer des ordonnances et des directives de cybersécurité; et
g. OREN 007 – Assurer la défense du cyberdomaine du MDN et des FAC.

3.6 Des tâches non-militaires particulières, propres au personnel responsable de la cyberdéfence et de la sécurité, ont été délibérément regroupées dans les OREN 001 à 005, et des tâches propres au MDN et aux FAC, dans les OREN 006 et 007. On cherche ainsi à faciliter la prestation des OREN 001 à 005 par l'entrepreneur.

4. ACRONYMES ET DOCUMENTS PERTINENTS

4.1 Acronymes

Les acronymes suivants sont utilisés dans le présent énoncé des travaux :

DF	Développement des forces
DG	Directeur général
EECFC	École d'électronique et des communications des Forces canadiennes
FAC	Forces armées canadiennes
GIGPM	Groupe d'instruction de la Génération du personnel militaire
MDN	Ministère de la Défense nationale

NQP	Norme de qualification et plan
OREN	Objectif de rendement
PSE	Protection, Sécurité, Engagement
QG de sdt	Qualification de grade soldat
RCN	Région de la capitale nationale
SCCM	System Centre Configuration Management
TI	Technologie de l'information

4.2 Documents pertinents

Les documents suivants, y compris toute modification, font partie du présent énoncé des travaux dans la mesure précisée aux présentes, et servent à l'étayer.

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. *Treasury Board Secretariat Guidelines to Ensuring Accessibility via Public Procurement* (Lignes directrices du Secrétariat du Conseil du Trésor visant à assurer l'accessibilité des marchés publics) [traduction libre] (http://www.gcpedia.gc.ca/gcwiki/images/5/57/Accessibility_in_Procurement_Guidance_-_April_2019-V1%28EN%29.pdf);
g. Guide de création de contenu pour le Réseau d'apprentissage de la Défense (https://www.canada.ca/fr/ministere-defense-nationale/services/avantages-militaires/education-formation/perfectionnement-professionnel/reseau-apprentissage-defense.html);
h. Volumes du système de l'instruction individuelle et d'éducation des Forces canadiennes, série de publications A-P9-050-000/PT001 (http://cda.mil.ca/pub/lib-bib/cfites-fra.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. DAOD 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. DOAD 5516-5, Mesures d'adaptation pour trouble d'apprentissage lors du recrutement, de l'instruction et de l'éducation (https://www.canada.ca/fr/ministere-defense-nationale/organisation/politiques-normes/directives-ordonnances-administratives-defense/serie-5000/5516/5516-5-mesures-adaptation-pour-trouble-apprentissage-lors-du-recrutement-de-instruction-et-de-education.html);
m. Ordonnances et directives de sécurité de la Défense nationale, chapitre 6 : sécurité de l'information (http://national.mil.ca/fr/sante-surete-securite/securite-politiques-odsdn.page);
n. Appendice 1, Qualification de grade soldat cyberopérateur;
o. Appendice 2, Objectifs de rendement et objectifs de compétence; et
p. Appendice 3, Liste des références.

5. PORTÉE

5.1 Le poste de cyberopérateur nécessite que de 12 à 24 participants soient formés par année pour respecter les exigences opérationnelles. Il s'agit d'un contrat initial d'une durée de deux ans comportant une séance de programme pour la prestation d'un cours pilote de cyberopérateur ainsi que quatre séances de programme optionnelles d'une durée de 17-mois.

5.2 Le temps requis pour l'exécution des OREN 001 à 005 devrait être d'environ 15 mois, ou quatre semestres de 15 semaines chacun. Voici les séances de programme requises :

a. période du contrat : août 2020 à décembre 2021;
b. période optionnelle 1 : août 2021 à décembre 2022;
c. période optionnelle 2 : août 2022 à décembre 2023;
d. période optionnelle 3 : août 2023 à décembre 2024;
e. période optionnelle 4 : août 2024 à décembre 2025.

6. EXIGENCES EN MATIÈRE DE FORMATION

6.1 L'entrepreneur doit démontrer que son programme est accrédité par une organisation de gouvernance et d'accréditation des études supérieures d'un gouvernement provincial dans le domaine de l'analyse de la cybersécurité (lié aux carrières civiles) ou des opérations de cybersécurité[1]. De plus, il doit réaliser les tâches suivantes :

a. Élaborer un programme de formation qui satisfera aux exigences en matière de rendement professionnel pour les OREN 001 à 005 du poste de cyberopérateur, grade de soldat, indiqués à l'appendice 1;

b. Faire évaluer et approuver le matériel didactique (à l'exception des plans de leçon) par le FAC-ACE (http://www.caface-rfacace.forces.gc.ca/fr/index). Ces activités peuvent lui prendre jusqu'à trois semaines. Pour se connecter, l'entrepreneur doit s'inscrire afin d'obtenir un compte du FAC-ACE. S'il éprouve des difficultés, il doit communiquer avec l'administrateur du système du FAC-ACE;

c. Tenir à jour le programme de formation, y compris tout le matériel didactique (plans de leçon, manuels, évaluations, cahiers de travail, etc.) en vue de satisfaire aux exigences en matière de rendement professionnel pour les OREN 001 à 005 du poste de cyberopérateur, grade soldat, indiqués à l'appendice 1, pendant toute la durée du contrat. Afin que ce contrat demeure à jour, il faut réviser en intégralité le matériel didactique tous les deux ans, à moins que celui-ci n'ait été rédigé il y a moins de deux ans, de sorte qu'il tienne compte des pratiques exemplaires actuelles dans le domaine de la cybersécurité; et

d. Soumettre toutes les modifications à apporter au matériel didactique (à l'exception des plans de leçon), aux fins d'évaluation et d'approbation au bureau de programme du FAC-ACE.

6.2 L'entrepreneur doit offrir 37,5 heures de formation par semaine et veiller au respect des heures établies pour la journée de formation standard en fonction du calendrier convenu. L'horaire de formation hebdomadaire doit comprendre :

a. un total de 27,5 heures de cours (temps d'apprentissage prévu au programme);
b. cinq pauses-repas d'une heure chacune;
c. trois périodes d'une heure destinées le conditionnement physique (au début ou à la fin de la journée de formation); et
d. une période de deux heures destinées aux tâches administratives personnelles.

[1] Les cyberopérations comprennent les cyberopérations défensives, offensives et de soutien, conformément à la note de doctrine interarmées (NDI) 2017-02 des FAC.

6.3 L'entrepreneur doit être reconnu en tant qu'établissement délivrant des diplômes d'études postsecondaires par une autorité éducative canadienne reconnue par la province. De plus, il doit conserver cette reconnaissance tout au long du contrat.

6.4 L'entrepreneur doit remettre aux participants ayant achevé le programme de formation pour le poste de cyberopérateur, grade soldat, un diplôme reconnu par la province en analyse de la cybersécurité ou en analyse de la défense du réseau.

6.5 L'entrepreneur doit fournir un centre de formation et des installations situés dans les limites géographiques de Kingston (Ontario) ou dans la région de la capitale nationale.

6.6 Le gouvernement du Canada s'efforce de veiller à ce que les biens et services qu'il achète soient inclusifs 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*. La DOAD 5516-5, Mesures d'adaptation pour trouble d'apprentissage lors du recrutement, de l'instruction et de l'éducation, précise les mesures d'adaptation à prendre pour l'instruction et l'éducation si un participant ayant un trouble d'apprentissage a besoin que de telles mesures soient prises.

7. MÉTHODE DE FORMATION

7.1 L'entrepreneur doit fournir une formation et des évaluations des participants qui sont axées sur les connaissances et compétences requises pour atteindre les OREN 001 à 005 décrits à l'appendice 1.

7.2 L'entrepreneur doit incorporer des séances de travail pratique pendant la formation pour que les participants développent leurs compétences relatives aux systèmes d'exploitation et applications logicielles d'analyse réseau fréquemment utilisés dans les secteurs public et privé, de même que dans les cyberopérations des FAC. Ces systèmes d'exploitation comptent notamment les postes de travail et serveurs Linux et Windows et les logiciels destinés aux utilisateurs, Apache, PHP, MySQL, Adobe, Microsoft Office et Wireshark. En outre, l'entrepreneur doit intégrer dans le matériel didactique des logiciels de script comme Python et Ruby, des outils d'analyse de logiciels malveillants comme Cuckoo Sandbox et des logiciels de configuration comme System Centre Configuration Management (SCCM), comme l'indique l'EECFC.

7.3 L'entrepreneur doit s'assurer que tous les examens, les documents et la formation sont offerts dans les deux langues officielles du Canada et fournis aux participants dans la langue de leur choix.

7.4 L'entrepreneur doit offrir une formation qui respecte les pratiques et normes des collèges communautaires provinciaux déterminées par l'autorité provinciale responsable de l'approbation des établissements d'enseignement (p. ex., le Conseil des universités de l'Ontario).

7.5 L'entrepreneur doit appliquer les procédures, normes et pratiques d'évaluation des participants des collèges communautaires tels qu'approuvés par la province. Il doit informer l'authorité technique dès que possible de tout participant qui risque de ne pas être en mesure de poursuivre le programme ou de le réussir, et ce, avant la fin du cours et avant le retrait de ce participant du programme. L'authorité technique examinera la situation scolaire du participant et transmettra toutes les dispositions nécessaires à l'entrepreneur par courriel. À noter que l'authorité technique peut réaliser d'autres évaluations des participants (p. ex., demander une deuxième opinion ou donner une deuxième chance au participant).

7.6 L'EECFC peut surveiller toute séance de formation ou d'évaluation en avisant l'entrepreneur par écrit. Des commentaires relatifs à la surveillance de la séance seront par la suite transmis à l'entrepreneur et à l'authorité technique par courriel.

7.7 L'entrepreneur doit au besoin offrir de l'encadrement, conformément aux procédures convenues par écrit avec l'EECFC. Ces dispositions doivent être transmises à l'EECFC au plus tard 30 jours ouvrables avant le début du programme. L'entrepreneur ou l'EECFC peut modifier ces dispositions, mais uniquement en consultation avec l'autre partie et avec le consentement écrit de celle-ci par courriel.

7.8 À la demande du responsable technique, l'entrepreneur doit fournir un exemplaire de tous les travaux cotés des participants. Les documents de formation de nature délicate doivent être protégés conformément aux points A2 à A4 à l'appendice 3.

7.9 L'entrepreneur doit fournir à l'autorité technique un relevé de notes final pour chaque participant dans les 30 jours ouvrables suivant l'achèvement ou l'abandon du programme de formation. Ces documents doivent être protégés conformément aux points A2 à A4 de l'appendice 3.

8. CALENDRIER DE FORMATION

8.1 L'entrepreneur doit fournir à l'autorité technique une copie numérique du calendrier de formation préliminaire en format Microsoft Word dans les 10 jours ouvrables suivant l'octroi du contrat. Il doit travailler avec l'authorité technique pour peaufiner le calendrier proposé afin de définir la durée du cours et le déroulement des journées de formation, de façon à répondre aux exigences des OREN et aux besoins des FAC. Le calendrier définitif doit être approuvé par l'authorité technique et publié par l'entrepreneur au moins 30 jours ouvrables avant le début de l'instruction.

8.2 Le calendrier de formation préliminaire doit indiquer clairement toutes les séances d'apprentissage pratiques et théoriques. À des fins de planification initiale, l'horaire quotidien doit être de 8 h à 16 h.

8.3 Le programme de formation des cyberopérateurs doit être achevé dans un délai de 15 mois avec un maximum de quatre semestres consacrés aux activités d'appentissage. Les semestres sont définis comme suit :

a. premier semestre – de septembre à décembre;
b. deuxième semestre – de janvier à avril;
c. troisième semestre – de mai à juillet; et
d. quatrième semestre – de septembre à décembre.

9. CENTRE DE FORMATION ET SOUTIEN SUPPLÉMENTAIRE

9.1 L'entrepreneur doit fournir un centre de formation et des installations conformes aux pratiques et normes des collèges communautaires de l'Ontario pour ce type de programme d'apprentissage. La salle de classe ou le laboratoire informatique doit offrir suffisamment d'espace pour tous les participants, le mobilier, le matériel ainsi que tous les appareils de TI et les logiciels communs nécessaires à la réalisation des OREN 001 à 005.

9.2 S'il y a lieu, l'entrepreneur doit fournir un accès au centre de formation et aux installations aux fins de réalisation d'activités supplémentaires de soutien et d'exercice des participants (supervisées ou non) à l'extérieur des heures de formation normales.

9.3 L'entrepreneur doit préparer et fournir du matériel didactique à jour en format électronique, en plus de fournir une version papier de tout manuel nécessaire à l'atteinte des OREN 001 à 005.

9.4 L'entrepreneur doit fournir une seule copie papier de tout manuel ou matériel de formation à chaque participant et au moins une copie papier à l'EECFC. Les manuels achetés par le MDN demeureront sa propriété.

9.5 L'entrepreneur doit fournir tout matériel de formation consommable, notamment les cahiers de travail et les documents à distribuer. Cela ne comprend pas les fournitures individuelles consommables des participants (p. ex., des fournitures qui peuvent être différentes entre les participants et que ceux-ci utilisent pour faciliter leur apprentissage, comme du papier, des stylos et crayons, divers articles de papeterie, etc.).

9.6 L'entrepreneur doit fournir un accès à la salle de classe ou au laboratoire informatique équipé de matériel périphérique pour les cyberopérations, ainsi que d'une configuration du réseau de soutien à l'information à tous les participants.

9.7 L'entrepreneur doit fournir de l'équipement de TI, des ressources de soutien et un réseau qui offre un accès à Internet, des comptes de courriel individuels pour les participants dotés d'un espace de stockage d'au moins 1 Go, un compte d'espace Web avec un espace de stockage d'au moins 5 Go ainsi qu'un accès à distance à son réseau des participants. La salle de classe ou le laboratoire informatique doit comprendre tout le matériel de TI nécessaire au respect des exigences des OREN 001 à 005 pour la formation des cyberopérateurs, en plus de comprendre des systèmes de sauvegarde convenables connectés au réseau afin d'assurer l'intégrité des données et du travail des participants.

9.8 Tout le matériel informatique doit être recyclé aux quatre ans, tout au plus, aux frais de l'entrepreneur.

9.9 Il faut purger tout l'équipement de TI prêté (ordinateurs portatifs, disques durs, etc.) à la fin du programme de formation ou avant de le retourner à un tiers, conformément aux politiques de sécurité de la TI du MDN A2 à A4, indiquées à l'appendice 3.

9.10 L'entrepreneur doit fournir une infrastructure de serveur et de réseau à l'appui des objectifs de formation qui respecte les exigences canadiennes en matière de traitement et d'entreposage des renseignements personnels des membres des FAC décrites au chapitre 6 des Ordonnances et directives de sécurité de la Défense nationale, portant sur la sécurité de l'information. L'entrepreneur et ses ressources doivent remplir et signer l'entente de non-divulgation s'ils ont besoin d'accéder aux renseignements personnels.

9.11 L'entrepreneur doit fournir les logiciels suivants pour la salle de classe ou le laboratoire informatique :

a. des systèmes d'exploitation couramment utilisés dans l'industrie (Linux ou Windows pour client et serveur);
b. des logiciels couramment utilisés dans l'industrie (Apache, PHP, MySQL, Adobe, Microsoft Office et Wireshark);
c. des logiciels de script couramment utilisés dans l'industrie (Python et Ruby);
d. des outils d'analyse de logiciels malveillants couramment utilisés dans l'industrie (Cuckoo Sandbox et InetSim); et
e. un logiciel de configuration (SCCM).

9.12 L'entrepreneur doit assurer la coordination de l'application des mises à niveau logicielles. Il doit déterminer le moment idéal pour réaliser cette opération de façon à minimiser l'incidence sur les cours. En outre, il doit coordonner les modifications à apporter aux plans de leçon du matériel de formation disponible, associées à la nouvelle version du logiciel. Par mise à niveau logicielle, on entend des modifications apportées à un logiciel existant qui sont diffusées sous un même numéro de version.

9.13 L'entrepreneur doit fournir à l'autorité technique des preuves d'ententes ou de licences pour les logiciels et le matériel par courriel dans les 60 jours civils précédant la date de début du programme de formation.

9.14 L'entrepreneur doit offrir un espace de bureau qui convient aux visites du personnel de l'EECFC et qui comprend des bureaux individuels pour deux membres du personnel de l'EECFC ainsi qu'une salle privée servant à la réalisation de consultations ou d'entrevues. Les bureaux doivent être meublés conformément aux pratiques et normes pour le personnel de formation des collèges communautaires de l'Ontario. Ils doivent comprendre, à tout le moins, deux téléphones individuels et un accès à des lignes de communication de données. S'il y a lieu, il doit fournir l'accès à ces installations pour des activités supplémentaires de soutien et d'exercice des participants à l'extérieur des heures de formation normales.

9.15 L'entrepreneur doit fournir au moins un réfrigérateur qui permet aux participants d'entreposer leurs repas de façon sécuritaire au cours de la journée, à savoir deux repas par jours pour 24 participants.

9.16 L'entrepreneur doit fournir un four à micro-ondes permettant aux participants de réchauffer leurs repas de façon sécuritaire.

9.17 L'entrepreneur doit fournir une aire de repas (distincte de la salle de classe ou du laboratoire informatique) pour que les participants puissent prendre leur repas en groupe. Celle-ci doit pouvoir accueillir tous les participants en même temps (il se peut que tous les participants doivent manger au même moment si on n'accorde qu'une seule période de dîner).

9.18 L'entrepreneur doit fournir un photocopieur (ainsi que différents formats de papier, de la poudre d'encre, des cartouches d'encre, etc.) aux fins d'utilisation des participants, sans frais pour ceux-ci ni pour le Canada.

10. EXIGENCES RELATIVES AUX RESSOURCES

10.1 Ressources

L'entrepreneur doit fournir les ressources suivantes en vue de satisfaire pleinement aux exigences du programme de formation de cyberopérateur, notamment :

a. un superviseur de contrat, aux fins de gestion du contrat et des questions connexes;
b. un coordonnateur de programme pour l'exécution du programme et la supervision des ressources contractuelles;
c. des professeurs qualifiés, selon un ratio participant et professeur de 12:1;
d. des formateurs (ou assistants), selon un ratio participant et instructeur ou assistant de 12:1;
e. des techniciens en TI, qui doivent assurer la viabilité des systèmes de soutien de la TI et du soutien technique pour les participants. Tout retard causé par des défectuosités techniques, la maintenance du système de TI ou des circonstances imprévues doit être couvert par l'entrepreneur sans coûts supplémentaires pour le Canada, de sorte que toutes les heures de formation hebdomadaires soient offertes aux participants, conformément à la section 6.2; et
f. toute autre ressource jugée nécessaire et appropriée en vue d'appuyer d'autres aspects de ce contrat (p. ex., des ressources de nettoyage pour maintenir l'hygiène des aires de repas).

10.2 Compétences obligatoires minimales

Les ressources doivent respecter les qualifications obligatoires minimales pour leur catégorie de ressource respective.

a. Les professeurs qualifiés doivent posséder :
   i. au moins quatre ans d'expérience; et
   ii. une maîtrise en informatique, notamment en programmation, en science de l'information ou en génie informatique, délivrée par une université, un collège ou une école secondaire reconnu du Canada, ou un diplôme équivalent tel qu'établi par un service canadien d'évaluation des titres de compétences reconnu (https://www.cicdi.ca/1/accueil.canada) si le diplôme a été obtenu à l'extérieur du Canada;

b. Les formateurs ou assistants doivent posséder :
   i. au moins trois ans d'expérience de formation dans le domaine lié aux OREN et aux objectifs de compétence (OCOM) connexes indiqués à l'appendice 1; et
   ii. un baccalauréat en informatique, notamment en programmation, en science de l'information ou en génie informatique, délivré par une université, un collège ou une école secondaire reconnu du Canada, ou un diplôme équivalent tel qu'établi par un service canadien d'évaluation des titres de compétences reconnu (https://www.cicdi.ca/1/accueil.canada) si le diplôme a été obtenu à l'extérieur du Canada.

11. EXIGENCES LINGUISTIQUES

11.1 L'entrepreneur et ses ressources doivent maîtriser (compréhension de l'oral et de l'écrit et expression orale et écrite) au moins une des langues officielles du Canada (anglais ou français). La maîtrise correspond au niveau 8 des *Canadian Language Benchmarks* pour l'anglais et des Niveaux de compétence linguistique canadiens pour le français (https://www.language.ca/apercu-des-niveaux-de-competence-nclc-et-clb/).

11.2 L'entrepreneur doit posséder un processus d'assurance de la qualité établi qui porte sur la correspondance et les produits livrables en anglais et en français, y compris un service de correction d'épreuves de toute la correspondance et des produits livrables.

11.3 Le Canada se réserve le droit de demander à l'entrepreneur d'évaluer les compétences linguistiques de ses ressources pendant la période du contrat, sans frais supplémentaires pour le Canada, au moyen de l'une des évaluations linguistiques approuvées par Immigration, Réfugiés et Citoyenneté Canada. Si une évaluation 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 frais encourus par l'entrepreneur et ses ressources pour les réunions ne seront pas remboursés à l'entrepreneur ni à ses ressources.

12.1 Réunion initiale

a. Une réunion initiale se tiendra dans les cinq jours ouvrables suivant l'attribution du contrat. Elle doit avoir lieu dans la région de la capitale nationale ou par téléconférence. L'heure et l'emplacement exacts de cette réunion seront convenus d'un commun accord entre l'entrepreneur et l'authorité technique;

b. Elle servira à :
   i. examiner les exigences contractuelles; et
   ii. examiner et préciser, s'il y a lieu, les rôles et responsabilités respectifs de l'EECFC, du GIGPM, du responsable technique et de l'entrepreneur afin d'assurer leur compréhension commune.

12.2 Réunions mensuelles

a. Le superviseur de contrat et le coordonnateur de programme de l'entrepreneur doivent participer à des réunions d'orientation de la formation à Kingston ou par téléconférence avec l'EECFC pour évaluer l'état du cours ainsi que la progression des participants. Celles-ci auront lieu au plus une fois par mois, à moins d'une entente entre l'entrepreneur et l'établissement de formation. La date et l'heure seront convenues entre l'entrepreneur et l'autorité technique; et

b. L'entrepreneur est chargé de préparer les ordres du jour et les comptes rendus de décisions de toutes les réunions. Il doit distribuer les ordres du jour cinq jours ouvrables avant les réunions, en plus de fournir à l'autorité technique les versions provisoires des comptes rendus de décisions dans les trois jours ouvrables suivant la réunion, à des fins d'examen.

13. LIMITES ET CONTRAINTES

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 se limiter à formuler des commentaires et des recommandations sur ces questions à l'autorité technique.

13.2 Les ressources de l'entrepreneur appelées à fournir les services ne relèvent pas directement des fonctionnaires du Canada et ne constituent d'aucune façon des employés ou des fonctionnaires du Canada.

13.3 Tout au long du contrat, l'entrepreneur ou ses ressources ne doivent pas ordonner à une organisation ministérielle ni au personnel d'un tiers avec lequel le Canada a conclu ou a l'intention de conclure un contrat, d'exécuter une action particulière.

13.4 Tout au long de la période de prestation des services requis, les ressources de l'entrepreneur n'auront accès à aucun renseignement exclusif, notamment à aucune donnée financière (y compris les prix unitaires ou les tarifs) ou technique relative à tout tiers avec lequel le Canada a conclu ou entend conclure un contrat, à l'exception de l'information relevant du domaine public (p. ex., la valeur totale du ou des contrats attribués). Des renseignements exclusifs peuvent être fournis aux ressources de l'entrepreneur dans le cadre de la prestation des services si elles ont rempli et signé une entente de non-divulgation.

13.5 Tous les dessins, les codes de logiciel, les rapports, les données, les documents ou le matériel fournis à l'entrepreneur par le Canada ou produits par les ressources de l'entrepreneur dans le cadre de la prestation des services prévus dans le contrat ne doivent servir qu'à répondre aux exigences dudit contrat. L'entrepreneur doit protéger les renseignements et les documents précités contre toute utilisation non autorisée et il ne doit pas les divulguer à des tiers, personnes ou organismes qui ne font pas partie du MDN, sans le consentement exprès écrit de l'organisation en cause (telle qu'identifiée à la section 3.4) ou de l'autorité technique. Ces renseignements et documents doivent être retournés à l'organisation respective ou à l'autorité technique à sa demande ou lorsque les services ont été menés.

13.6 Toute la correspondance, qu'elle provienne des ressources de l'entrepreneur ou de toute section du MDN, doit être soumise à l'organisation respective ou a l'autorité technique. Il peut s'agir notamment d'enregistrements des conversations, de comptes rendus des décisions et de correspondance écrite dans quelque format que ce soit.

13.7 L'authorité technique ou l'organisation respective doit avoir accès en tout temps aux travaux et aux installations où on exécute une partie du travail.

13.8 L'entrepreneur doit veiller à ce que ses ressources n'utilisent pas les appellations, les logos, ni les emblèmes du gouvernement du Canada ou du MDN sur les cartes professionnelles, les panneaux posés sur les postes de travail modulaires, dans les bureaux ou dans la correspondance imprimée et électronique de manière à ce que ces personnes soient perçues comme des employés du gouvernement du Canada.

Appendice 1

Qualification au grade de soldat cyberopérateur

Liste des abréviations

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

Aperçu de l'exigence de formation : Les cyberopérateurs effectuent des opérations défensives de réseau et informatiques et assurent une liaison avec les alliés du Canada afin d'améliorer les capacités du MDN et des FAC leur permettant d'offrir un cyberenvironnement 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 celles-ci. Ils fournissent aussi un cyberappui afin de combler les besoins opérationnels de la Marine, de l'Armée et de l'Aviation. Les cyberactivités et les cybertâches offensives, qui comprennent la perturbation des actions de l'adversaire dans le cyberdomaine, font aussi partie de la portée de leur travail. Cette instruction vise à préparer les cyberopérateurs à effectuer les tâches de l'emploi de premier échelon de « CYBEROP ». Ce travail est effectué dans un centre d'opérations à l'appui des éléments maritime, terrestre et aérien. La principale responsabilité est d'identifier des indicateurs de compromission par l'analyse des réseaux du MDN et des FAC. Les tâches principales sont : rassembler, examiner et analyser les cyberalertes, ainsi que produire des rapports techniques sur les cyberalertes.

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

Module 1 – OREN 001 à 005 (principal objectif de cette exigence de formation, énumérés ci-dessous) : À être offert par l'entrepreneur.

Module 2 – OREN 006 et 007 (ne sont pas inclus dans la présente exigence de formation) : À être offert par un établissement de formation des FAC. L'objectif de ces OREN est que le cyberopérateur applique les compétences génériques et les techniques de surveillance du réseau élaborées dans les OREN 001 à 005 dans un contexte des FAC.

OREN et OCOM connexes :

OREN 001 – Maintenir une connaissance de la situation du réseau : L'intention de cet OREN est de préparer le cyberopérateur à mener des activités pour 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 de réseau et en étalonnant le trafic du réseau, le cyberopérateur doit bien connaître les technologies, l'architecture, les appareils et les communications du réseau. En dirigeant les évaluations de vulnérabilité, il doit connaître les vulnérabilités, les menaces et les vecteurs d'attaque courants afin de les analyser et de conseiller des mesures d'atténuation.

De plus, il doit avoir une compréhension générale des divers systèmes d'exploitation (ordinateur et serveur), de la virtualisation et des divers autres secteurs du réseautage et des technologies de l'information (TI) afin de déterminer si des anomalies ont été détectées pendant une analyse du réseau ou pendant des captures 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 : L'intention de cet OREN est de préparer le cyberopérateur à faire enquête sur un événement au moyen de données recueillies à l'aide d'un ensemble d'outils de cyberdéfense (p. ex., alertes du système de détection d'intrusion (SDI), pare-feu, registres du trafic du réseau). Le cyberopérateur 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 : L'intention de cet OREN est de préparer le cyberopérateur à produire un rapport à l'aide de toutes les données brutes disponibles, à compléter les analyses et les autres rapports pertinents ainsi que 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 : L'intention de cet OREN est de préparer le cyberopérateur à configurer le matériel et le logiciel. Le cyberopérateur sera capable d'installer, de maintenir et de retirer le matériel et les logiciels de cyberdéfense, et de créer et retirer des règles du système de détection d'intrusion / système de protection contre les intrusions (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 uniques. 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 du matériel des outils
OCOM 004.06 — Faire le dépannage des défaillances des logiciels 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 : L'intention de cet OREN est de préparer le cyberopérateur à concevoir, créer, tester et maintenir des outils logiciels personnalisés. Il pourra déterminer les défaillances des outils existants afin de concevoir et de créer des outils pour résoudre ces défaillances. Il doit posséder des compétences en rédaction de scripts et doit pouvoir écrire des petits programmes afin de créer des outils personnalisés. Cet OREN n'a pas pour objectif de faire du cyberopérateur un expert en développement logiciel, mais il lui donnera des compétences de base en rédaction de scripts et des compétences de base pour les autres OREN, ainsi que pour des formations spécialisées futures basées sur l'emploi.

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

Voir l'appendice 3 pour une liste des références aux OCOM codée de façon alphanumérique (C1, C2, C3, etc.).

OREN 001 – Maintenir une connaissance de la situation du réseau

OCOM	Contenu de l'OCOM (ce que les participants doivent être capables de faire à la fin de la formation)
OCOM 001.01 – Énumérer un réseau et un système	(1) Préparer l'outil d'analyse réseau, notamment : (a) identifier les objectifs et l'espace IP; (b) vérifier les objectifs et l'espace IP comme propriété du MDN/des FAC; (c) configurer l'outil d'analyse réseau, conformément aux documents sur l'outil. (2) Faire l'essai d'une fonctionnalité d'évaluation de réseau personnalisé, ce qui comprend : (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 relatifs à 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 comprend : (a) lancer et surveiller la progression de l'analyse; (b) effectuer le dépannage de la progression de l'analyse et en assurer la reconfiguration, ce qui comprend la pause, l'évaluation des résultats, la modification et la reprise de l'analyse; (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, notamment : (a) relever l'information essentielle, ce qui comprend : i. nommer les applications et SE d'un dispositif, ii. cerner d'autre information, notamment le type de dispositif, l'état du port, l'IP, le nom de l'hôte, etc.; (b) prendre les empreintes numériques du dispositif, ce qui comprend : 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 comprend : i. désigner l'emplacement à l'aide d'outils automatisés (p. ex., IP Control) ou d'autres outils de surveillance réseau,

OCOM	Contenu de l'OCOM (ce que les participants doivent être capables de faire à la fin de la formation)
	ii. désigner l'emplacement à l'aide d'autres méthodes, comme vérifier la géolocalisation d'autres adresses IP à portée, faire des références croisées avec des données d'analyse antérieures et faire des références croisées avec 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 l'analyse automatisée; (c) aux organisations partenaires. (2) Créer une carte de réseau, ce qui comprend l'utilisation de : (a) méthodes manuelles pour créer la carte (p. ex., Microsoft Visio, Microsoft PowerPoint) ou d'autres moyens; (b) méthodes automatisées pour créer la carte, ce qui comprend les outils automatisés (p. ex., ZenMap, LanState Pro) et les 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 à la documentation.
OCOM 001.03 – Cerner les vulnérabilités du réseau et du système	(1) Préparer des outils d'évaluation des vulnérabilités et une méthodologie d'évaluation, notamment : (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) vérifier les objectifs et l'espace IP comme propriété du MDN ou des FAC; (d) acquérir les droits administratifs ou l'équivalent pour atteindre les résultats de l'analyse; (e) configurer l'outil d'évaluation des vulnérabilités, conformément aux documents sur l'outil. (2) Faire l'essai d'une fonctionnalité d'évaluation de réseau personnalisé, ce qui comprend : (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 relatifs à l'utilisation de la bande passante, la durée d'exécution de l'analyse ou d'autres paramètres. (3) Effectuer une évaluation de la vulnérabilité fondée sur des outils, notamment : (a) lancer et surveiller la progression de l'analyse; (b) effectuer le dépannage de la progression de l'analyse et en assurer la reconfiguration, ce qui comprend la pause, l'évaluation des résultats, la modification et la reprise de l'analyse; (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.

OCOM	Contenu de l'OCOM (ce que les participants doivent être capables de faire à la fin de la formation)
	(4) Effectuer une évaluation manuelle de la vulnérabilité, notamment : (a) assurer la liaison avec des experts en la matière, des administrateurs de systèmes, des opérateurs de systèmes, le personnel technique, 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, notamment : (a) examiner les scores de gravité des résultats automatisés (p. ex., les scores sur les CVE); (b) effectuer une évaluation combinée des résultats manuels et automatisés; (c) évaluer l'incidence et la probabilité d'exploitation de toutes les vulnérabilités découvertes. (6) Amorcer la production de 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.

OREN 002 – Réagir à un cyberévénement

OCOM	Contenu de l'OCOM (ce que les participants doivent être capables de faire à la fin de la formation)
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, notamment : (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 de l'alerte, conformément aux références C76, C99, C105, C106 et C107; (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, notamment : (a) analyser les anomalies dans le trafic du réseau à l'aide des métadonnées, conformément aux références C57 et C125; (b) relever la carte du réseau et les empreintes numériques du système d'exploitation; (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	Contenu de l'OCOM (ce que les participants doivent être capables de faire à la fin de la formation)
COM 002.02 – Enquêter sur des cyberévénements	(1) Valider les alertes/comportements anormaux par l'analyse du réseau, notamment : (a) recueillir les métadonnées, les données de trafic et les registres, ce qui comprend : i. déterminer les applications et les SE d'un dispositif selon le trafic du réseau, conformément aux références C58, C78, C97, C116, C118 et C125, ii. déterminer le calendrier 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, iv. déterminer l'emplacement des ressources physiques du réseau, conformément aux références C125, C127 et C128; (b) reconstituer les activités malveillantes, notamment : 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. cerner 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 des hôtes, ports). (2) Effectuer l'analyse de la capture des paquets de données, notamment : (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; (c) rassembler les artefacts, conformément à la référence C74. (3) Effectuer l'analyse du maliciel, conformément aux références C74, C77 et C95, ce qui comprend : (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 participants doivent être capables de faire à la fin de la formation)
OCOM 002.03 – Produire des rapports internes	(1) Regrouper des données pertinentes pour produire un rapport technique, notamment : (a) déceler ou reconnaître l'événement ou le problème; (b) créer une ligne de temps étayée de l'incident; (c) indiquer les conclusions et les résultats pertinents qu'il faut communiquer au superviseur, à l'organisme externe ou au client; (d) déterminer 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 tous renseignements généraux; (b) les observations/résultats (risques et vulnérabilités, conclusions des analyses, faits reliés aux systèmes et au réseau/aux données); (c) les conclusions tirées en se fondant sur les observations et les constatations; (d) la recommandation de mesures d'atténuation pour améliorer la sécurité ou recommander des mesures de récupération 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) Étayer en détail la nature de l'artefact. (4) Étayer de quelle façon il a été obtenu. (5) Étayer le moment où il a été recueilli. (6) Consigner le nom de la personne qui a traité l'artefact et étayer les mesures qui ont été prises. (7) Étayer l'endroit où l'artefact est entreposé.

OREN 003 – Produire un rapport technique

OCOM	Contenu de l'OCOM (ce que les participants doivent être capables de faire à la fin de la formation)
OCOM 003.01 – Regrouper des données pertinentes pour produire un rapport technique	(1) Déceler ou reconnaître l'événement ou le problème. (2) Créer une ligne de temps documentée de l'événement ou du problème. (3) Extraire les détails pertinents contenus dans les notes d'analyse du document. (4) Indiquer les conclusions et les résultats pertinents qu'il faut communiquer au superviseur, à l'organisme externe ou au client. (5) Déterminer les 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 tous renseignements généraux; (2) les observations/résultats (risques et vulnérabilités, conclusions des analyses, faits reliés aux systèmes et au réseau/aux données); (3) les conclusions tirées en se fondant sur les observations et les constatations; (4) recommander des mesures d'atténuation pour améliorer la sécurité ou recommander des mesures de récupération après l'incident; (5) toute nouvelle information pertinente relative à l'événement ou au problème qui peut améliorer l'exactitude du rapport.

OCOM	Contenu de l'OCOM (ce que les participants doivent être capables de faire à la fin de la formation)
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) la clarté (le rapport est explicite, détaillé, exhaustif, intelligible et sans ambiguïté); (2) l'exactitude (la justesse des détails et des faits du rapport); (3) la pertinence (le rapport ne contient pas de mots, d'expressions et d'idées non pertinents); (4) la concision (le rapport est concis, les idées et les faits sont exprimés avec le plus de concision possible sans nuire à la clarté, à la justesse ou à la pertinence); (5) la rapidité de la publication (le rapport est remis conformément aux délais requis).

OREN 004 – Préparer un environnement d'analyse

OCOM	Contenu de l'OCOM (ce que les participants doivent être capables de faire à la fin de la formation)
OCOM 004.01 – Installer le matériel requis	Installer le matériel requis, notamment : (1) poste de travail; (2) disque dur; (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) les routeurs; (2) les commutateurs; (3) les pare-feu; (4) les dispositifs TAP de réseau; (5) les SDI et les SPI.
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 comprend : (a) installer un poste de travail virtuel d'utilisateur Windows, conformément aux références C27 et C43; (b) installer différentes images virtuelles de postes de travail, conformément aux références C32 et C43; (c) installer différentes images virtuelles mobiles, conformément à la référence C129; (d) configurer des serveurs Windows, ce qui comprend : i. le contrôleur de domaines, conformément aux références C28, C29 et C30, ii. le serveur de fichiers et d'imprimantes, conformément aux références C28, C29 et C30, iii. le DNS, conformément aux références C28, C29, C30, C46 et C47, iv. le serveur DHCP, conformément aux références C28, C29 et C30, v. le serveur Exchange, conformément aux références C28, C29, C30 et C48, vi. le serveur Web Microsoft IIS, conformément aux références C28, C29 et C30, vii. le serveur MySQL, conformément aux références C28, C29 et C30.

OCOM	Contenu de l'OCOM (ce que les participants doivent être capables de faire à la fin de la formation)
	(2) Installer les politiques du groupe de 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 comprend : (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 TAP réseau; (d) les SPI; (e) les pare-feu, conformément aux références C49 et C56. (5) Gérer les instantanés des images virtuelles, conformément à la référence C43, ce qui comprend : (a) prendre des instantanés virtuels; (b) revenir à des anciens instantanés; (c) revenir à de nouveaux instantanés; (d) supprimer des instantanés. (6) Installer un environnement de poste de travail virtuel local (poste de travail Virtual Box ou VMware), ce qui comprend installer une image de SE virtuelle (format .iso), conformément à la référence C43.
OCOM 004.04 – Configurer un logiciel	(1) Installer des logiciels, ce qui comprend : (a) les logiciels d'utilisateur (Adobe, Office, Wireshark); (b) les logiciels de rédaction de scripts (Python, Ruby); (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 du matériel des outils	(1) Remplacer le matériel. (2) Configurer les réseaux physiques.
OCOM 004.06 – Faire le dépannage des défaillances des logiciels des outils	(1) Résoudre les défaillances du logiciel. (2) Désinstaller et installer des applications. (3) Installer et supprimer des correctifs.

OCOM	Contenu de l'OCOM (ce que les participants doivent être capables de faire à la fin de la formation)
OCOM 004.07 – Installer et maintenir les capteurs du réseau	(1) Installer un dispositif TAP réseau en ligne et hors bande, conformément à la référence C130, ce qui comprend : (a) installer un dispositif TAP matériel; (b) faire une écriture miroir du port commutateur (Hewlett Packard, CISCO). (2) Confirmer la fonctionnalité du capteur réseau, ce qui comprend : (a) vérifier la capture de l'ensemble des paquets, ce qui comprend la conservation de la capture de l'ensemble des paquets et le moment lorsque les paquets sont acheminés; (b) vérifier la conservation des métadonnées; (c) effectuer des vérifications des capteurs et signaler les pannes, ce qui implique notamment d'informer le superviseur de la fonctionnalité. (3) Élaborer des règles pour le capteur réseau, ce qui comprend : (a) rédiger une règle pour le capteur réseau; (b) faire l'essai de la fonctionnalité de la règle du capteur réseau; (c) recommander le déploiement des règles de capteur réseau; (d) télécharger les règles de capteur réseau dans les capteurs; (e) confirmer la validité des alertes du capteur réseau par rapport au trafic du réseau; (f) recommander la désactivation des règles de capteur réseau.
OCOM 004.08 – Désinstaller les logiciels et le matériel nécessaire	(1) Désinstaller les logiciels et le matériel nécessaires, ce qui comprend : (a) désinstaller les logiciels avec la fonction « ajouter/supprimer des programmes » dans Windows; (b) désinstaller les logiciels à partir de la ligne de commande Linux (« apt-get and yum remove »); (c) formater l'ordinateur (programme KillDisk). (2) Désinstaller le matériel requis (commutateur, routeur, dispositif TAP, USB, disque dur).

OREN 005 – Développer des outils logiciels

OCOM	Contenu de l'OCOM (ce que les participants doivent être capables de faire à la fin de la formation)
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) Transformer les exigences de sécurité en éléments de conception de l'application, ce qui comprend : (a) étayer les éléments des surfaces d'attaque des logiciels; (b) cerner les implications liées à la sécurité sur le réseau, conformément à la référence C16 (chapitre 8). (3) Préparer les tableaux de flux de travail, ce qui comprend : (a) mettre en œuvre des mesures de sécurité dans le cycle de développement des logiciels, conformément à la référence C17 (chapitres 3 à 5); (b) produire un tableau de flux de travail de programmation, conformément aux références C12, C14 (chapitre 12) et C15 (chapitres 13, 14 et 22).

OCOM	Contenu de l'OCOM (ce que les participants doivent être capables de faire à la fin de la formation)
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, notamment : (a) concevoir des algorithmes, ce qui comprend : 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; (b) appliquer les normes de code et d'essai, ce qui comprend les outils d'essai et la réalisation d'essais des programmes, ce qui comprend : i. le débogage des logiciels et les 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 s'assurer des bons résultats, conformément aux références C15 et C17.
OCOM 005.03 – Concevoir des outils logiciels	(1) Déterminer les correctifs logiciels appropriés et les étayer, conformément à la référence C41. (2) Modifier les logiciels existants, conformément aux références C14 (chapitres 17 et 18), C41 et C42 (chapitre 54), notamment : (a) corriger les erreurs; (b) mettre à jour les interfaces; (a) améliorer la performance. (3) Effectuer l'analyse des risques lorsqu'une application subit une modification profonde, conformément aux références C14, C41 et C42 (chapitre 54).

Appendice 3

Liste des références

Les références des OCOM à l'appendice 2 sont surlignées en jaune.

Référence	Publication
A	**Ouvrages de référence militaires canadiens**
A1	A-P2-002-NDA/PG-B01, Analyste de la défense du réseau – Norme de qualification et plan de formation
A2	ODSDN —Ordonnances et directives de sécurité de la Défense nationale, chapitres 6 et 7 (http://intranet.mil.ca/fr/sante-surete-securite/securite-politiques-odsdn.page).
A3	ODSDN —Ordonnances et directives de sécurité de la Défense nationale, chapitres 5, 6 et 7 (http://intranet.mil.ca/fr/sante-surete-securite/securite-politiques-odsdn.page).
A4	SMA(GI) – Politiques et normes de sécurité de la TI (http://admim-smagi.mil.ca/fr/securite/politiques-normes/index.page)
A5	A-SJ-100-002/AS-001, Sécurité des systèmes d'information — Normes de sécurité opérationnelle pour les systèmes d'information (NSOSI) (http://www.forces.gc.ca/fr/a-propos-politiques-normes-directives-ordonnances-administratives-defense-6000/6003-0.page)
A6	Introduction aux cyberopérations des FAC, février 2014, Chef — Développement des Forces
A7	NDI 2017-02, Note de doctrine interarmées des FAC – Cyberopérations
A8	DOAD 6002-2 (http://intranet.mil.ca/fr/directives-ordonnances-administratives-defense/6000/6002-2.page)
B	**Ouvrages de référence des forces alliées**
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	CIICS User Guide (guide de l'utilisateur du Système de coordination des incidents et de la cyberinformation)
C	**Ouvrages de référence commerciaux**
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 à l'algorithmique, 2e édition
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 9782841773503, 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
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)

Référence	Publication
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, 9e édition (examens 220-901 et 220-902)
C22	ISBN : 9780071848220, CompTIA Network+ All-In-One Exam Guide, 6e édition (examen N10-006)
C23	ISBN 9781119288282, CCNA Routing and Switching Complete Study Guide (examens 100—105, 200-105 et 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 – 2e édition
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, 6e édition
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
C49	ISBN : 9781587142727, Implementing Cisco IOS Network Security (IINS 640-554) Foundation Learning Guide (2e édition) (guides d'apprentissage de base)
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, examens 640-721 et 640-721
C53	ISBN 9788126543311, CCNA Data Center: Introducing Cisco Data Center Networking Study Guide, examen 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)

Référence	Publication
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, 3e édition
C57	ISBN 9781593275099, The practice of Network Security Monitoring: Understanding Incidence Detection and Response
C58	ISBN 9780471661863, Computer Networking – Internet Protocols in Action
C59	ISBN : 9780735712652, Network Intrusion Detection – 3e édition
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	Outils de validation de la légitimité d'un réseau d'alerte, y compris traceroute, nslookup, dig, whois, ping (http://centralops.net)
C76	Valider la légitimité d'adresses IP d'analyse d'alertes au moyen de multiples listes noires d'adresses IP et de DNS (http://ipvoid.com)
C77	Tcpdump/libcap (http://www.tcpdump.org)
C78	Aide mémoire (en-têtes, ports et protocoles) (http://packetlife.net/library/cheat-sheets/)
C79	RFC 1700 (numéros de ports) (https://www.ietf.org/rfc/rfc1700.txt)
C80	IANA (https://www.iana.org/)
C81	Liste de ports logiciels (https://fr.wikipedia.org/wiki/Liste_de_ports_logiciels)
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	Calculatrice de sous-réseau en ligne (http://www.subnet-calculator.com/)
C87	Jeu concernant les sous-réseaux de Cisco (https://learningnetwork.cisco.com/docs/DOC-1802)
C88	Présentation de Cisco au sujet des adresses IP et des sous-réseaux (approfondi) (http://www.cisco.com/c/en/us/support/docs/ip/routing-information-protocol-rip/13788-3.html)
C89	Guides sur IPv6 (https://ipv6.he.net/certification/primer.php) (https://fr.wikipedia.org/wiki/IPv6)
C90	Certification IPv6 (https://ipv6.he.net/certification/)
C91	Regex (https://support.sas.com/rnd/base/datastep/perl_regexp/regexp-tip-sheet.pdf)

Référence	Publication
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	Opérateurs de recherche Google (https://support.google.com/websearch/answer/2466433)
C97	Common Vulnerability Database (base de données sur les vulnérabilités fréquentes) (https://cve.mitre.org/)
C98	Validation de la légitimité d'une alerte, balayage des sites Web au moyen de multiples moteurs de réputation et listes noires (http://urlvoid.com)
C99	Validation de la légitimité d'une alerte, American Registry for Internet Numbers (http://arin.net)
C100	Validation de la légitimité d'une alerte, trousse d'outils Hurricane Electric Border Gateway Protocol (BGP) (http://bgp.he.net)
C101	Validation de la légitimité d'une alerte, Robtex Swiss Army Knife Internet Tool (http://www.robtex.com)
C102	Validation de la légitimité d'une alerte, sites Web de signatures d'alerte, Snort Rules Website and Rule Lookup (http://tools.cisco.com/security/center/search.x?search=Signature)
C103	Validation de la légitimité d'une alerte, sites Web de signatures d'alerte, Emerging Threats Snort Rule Database (http://doc.emergingthreats.net/)
C105	Validation de la légitimité d'une alerte, sites Web de signatures d'alerte, Snort Rules Website and Rule Lookup (https://snort.org/downloads/#rule-downloads)
C106	Sites Web de signatures 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	Foire aux questions sur la détection des intrusions (https://www.sans.org/security-resources/idfaq/are-there-limitations-of-intrusion-signatures/1/21)
C112	Guide sur les 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	Glossaire — SANS (www.sans.org/security-resources/glossary-of-terms)
C119	Page d'accueil PCAP (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	Guide de l'utilisateur de Sericata (http://suricata.readthedocs.io/en/latest)
C123	Documentation de Yara (http://yara.readthedocs.io/en/v3.4.0/index.html)
C124	Documentation de Stix (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)

Référence	Publication
C127	Géolocalisation d'adresse IP (http://www.ipfingerprints.com/)
C128	Géolocalisation d'adresse IP (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 (4e 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**
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/publications)
D3	ITSG-33, La gestion des risques liés à la sécurité des TI : une méthode axée sur le cycle de vie (CST) (https://www.cse-cst.gc.ca/fr/publication/itsg-33)
D4	*Loi sur la preuve au Canada* (https://laws-lois.justice.gc.ca/fra/lois/C-5/TexteComplet.html)
D5	RDDC CARO TM 2013-XXX, Military Activities and Cyber Effects (MACE) Taxonomy, décembre 2013 (http://cradpdf.drdc-rddc.gc.ca/PDFS/unc218/p803340_A1b.pdf)
D6	ITSB-120, Guide d'initiation à la sécurité interdomaines (https://www.cse-cst.gc.ca/fr/publication/list/Network-Security)
D7	ITSB-49, Bulletin de sécurité — Enregistreurs de frappe et logiciels espions (https://www.cse-cst.gc.ca/fr/publication/list/Network-Security)
D8	ITSG-41, Exigences de sécurité liées aux réseaux locaux sans fil (https://www.cse-cst.gc.ca/fr/publication/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://www.cse-cst.gc.ca/fr/publication/itsb-96)
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, version 3 - Les 10 mesures de sécurité des TI visant à protéger les réseaux Internet et l'information du gouvernement du Canada (https://www.cse-cst.gc.ca/fr/publication/list/Security-Protocols)
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* (L.R.C. [1985], ch. O-5) (http://laws-lois.justice.gc.ca/fra/lois/O-5/)

Référence	Publication
D14	*Code criminel* (L.R.C. [1985], ch. C-46) article 184 – Interception des communications (http://laws-lois.justice.gc.ca/fra/lois/C-46/page-41.html?txthl=communications+communication+interception+intercepted+intercept#s-184.2)
D15	*Code criminel* (L.R.C. [1985], ch. C-46) article 342.1 – Utilisation non autorisée d'ordinateur (http://laws-lois.justice.gc.ca/fra/lois/C-46/page-76.html?txthl=unauthorized+computer+use#s-342.1)
D16	*Code criminel* (L.R.C. [1985], ch. C-46) article 430(1.1) – Méfait à l'égard de données informatiques (http://laws-lois.justice.gc.ca/fra/lois/C-46/page-89.html?txthl=relation+relating+mischief+computer+data#s-430)
D17	CSE OPS-1 (document CLASSIFIÉ)
D18	CSE OPS 5-15 (document CLASSIFIÉ)
D19	CSE CSOI 4-1 (document CLASSIFIÉ)
D20	Normes canadiennes de sécurité en matière de SIGINT (document CLASSIFIÉ)
D21	IPO du CORFC — Physical Media Analysis — Forensics Taskings
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	CORFC, Ops Reference Guide
D25	CORFC, Surveillance Analyst Working Aide
D26	CORFC, Surveillance Report Template
D27	Notes de cours du Bref cours sur la sécurité des réseaux (BCSR), exposés 1 à 5 sur le réseau informatique
D28	Notes de cours du BCSR, exposés 1 à 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 à 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
W4938-20-069S

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: Department of National Defence	2. Branch or Directorate / Direction générale ou Direction Canadian Defence Academy
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 deliver and maintain a Cyber Op training program for CAF members

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)	___ 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)

TBS/SCT 350-103(2004/12)

Security Classification / Classification de sécurité
Unclassifed

Canada

Government of Canada / Gouvernement du Canada

Contract Number / Numéro du contrat
W4938-20_0695

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 ✓ / Yes
Le fournisseur aura-t-il accès à des renseignements ou à des biens COMSEC désignés PROTÉGÉS et/ou CLASSIFIÉS? — Non ✓ / Oui
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 ✓ / Yes
Le fournisseur aura-t-il accès à des renseignements ou à des biens INFOSEC de nature extrêmement délicate? — Non ✓ / Oui

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 ✓ / Yes
Du personnel sans autorisation sécuritaire peut-il se voir confier des parties du travail? — Non ✓ / Oui
If Yes, will unscreened personnel be escorted? — No / Yes
Dans l'affirmative, le personnel en question sera-t-il escorté? — Non / Oui

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 ✓ / Yes
Le fournisseur sera-t-il tenu de recevoir et d'entreposer sur place des renseignements ou des biens PROTÉGÉS et/ou CLASSIFIÉS? — Non ✓ / Oui

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

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 ✓ / Yes
Les installations du fournisseur serviront-elles à la production (fabrication et/ou réparation et/ou modification) de matériel PROTÉGÉ et/ou CLASSIFIÉ? — Non ✓ / Oui

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 ✓ / Yes
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? — Non ✓ / Oui

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

Government of Canada / Gouvernement du Canada

Contract Number / Numéro du contrat
W4938-20-0695

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	PROTECTED / PROTÉGÉ B	PROTECTED / PROTÉGÉ C	CONFIDENTIAL / CONFIDENTIEL	SECRET	TOP SECRET / TRÈS 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? — No ✓ / Yes
La description du travail visé par la présente LVERS est-elle de nature PROTÉGÉE et/ou CLASSIFIÉE? — Non / 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? — No ✓ / Yes
La documentation associée à la présente LVERS sera-t-elle PROTÉGÉE et/ou CLASSIFIÉE? — Non / 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 W4938-20069S/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 : W4938-20069S/001/ZH.

_____
Signature

_____
Date