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

SOLICITATION AMENDMENT
MODIFICATION DE L'INVITATION

The referenced document is hereby revised; unless otherwise indicated, all other terms and conditions of the Solicitation remain the same.

Ce document est par la présente révisé; sauf indication contraire, les modalités de l'invitation demeurent les mêmes.

Comments - Commentaires

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

Issuing Office - Bureau de distribution

Security and Information Operations Division/Division de la securite et des operations d'information
11 Laurier St. / 11, rue Laurier
8C2, Place du Portage
Gatineau
Québec
K1A 0S5

Title - Sujet CD-DAR - ISQ Invitation à se qualifier: Cyberdéfence – décision, analyse et réponse	
Solicitation No. - N° de l'invitation W6369-20CY06/C	**Amendment No. - N° modif.** 009
Client Reference No. - N° de référence du client W6369-20CY06	**Date** 2021-07-16
GETS Reference No. - N° de référence de SEAG PW-$$QE-049-28197	
File No. - N° de dossier 049qe.W6369-20CY06	**CCC No./N° CCC - FMS No./N° VME**

Solicitation Closes - L'invitation prend fin
at - à 02:00 PM Eastern Daylight Saving Time EDT
on - le 2021-07-28 Heure Avancée de l'Est HAE

F.O.B. - F.A.B.
Plant-Usine: ☐ **Destination:** ☑ **Other-Autre:** ☐

Address Enquiries to: - Adresser toutes questions à: Wight, Patti	**Buyer Id - Id de l'acheteur** 049qe
Telephone No. - N° de téléphone (873) 355-3543 ( )	**FAX No. - N° de FAX** ( ) -

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

Instructions: See Herein

Instructions: Voir aux présentes

Delivery Required - Livraison exigée	**Delivery Offered - Livraison proposée**

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

L'AMENDEMENT 009 EST SOULEVÉ POUR:

1. Répondre aux questions relatives à l'Invitation à se qualifier.
2. Modifier l'invitation à se qualifier comme indiqué ci-dessous.

Amendement 009-1

VOIR: Tableau 2 – Critères d'évaluation techniques cotés
SUPPRIMER: C3 dans son intégralité
INSÉRER :

C3	Le répondant a réussi la mise en œuvre, au cours des sept (7) dernières années, d'un (1) projet de GI/TI complexe comprenant la conception, le développement, l'intégration, la mise en œuvre de solutions commerciales, gouvernementales ou militaires standard intégrées de cybersécurité et d'analyse de décisions et de réponse cybernétique et de resynchronisation dans des pays du Groupe des cinq et de services de soutien à la stabilisation pendant au moins douze (12) mois pour tous les aspects suivants d'un réseau donné : (a) réseau distribué à l'échelle mondiale sur au moins deux (2) continents comportant au moins dix (10) nœuds opérationnels distincts, (b) interconnecté à distance à faible vitesse (liaisons de moins de 1,544 Mbps) dans des environnements austères à un réseau central à haute vitesse (100 Mbps ou plus), et (c) pour la transmission de données liées à la cybersécurité, un réseau de : i) de 2 001 à 4 000 dispositifs terminaux; ii) de 4 001 à 6 000 dispositifs terminaux; iii) de 6 001 à 8 000 dispositifs terminaux; iv) Plus de 8 000 dispositifs terminaux Pour le critère C3 (c), le projet du répondant doit inclure au moins cinq (5) des neuf (9) exemples de données et de renseignements liés à la cybersécurité ci-dessous : 1. Identification et suivi des actifs de GI/TI autorisés et non autorisés; 2. Renseignements relatifs à chacune des évaluations des vulnérabilités, de la configuration, des risques et de la conformité aux correctifs;	Les points seront accordés en fonction du nombre de dispositifs terminaux du projet. Nombre maximal : Vingt (20) points 5 points 10 points 15 points 20 points		Le répondant doit fournir au plus une (1) référence d'un projet exécuté au cours des sept (7) dernières années où il a mis en place une solution d'analyse et de réponse de cybersécurité et de cyberdécision intégrée de matériel commercial, gouvernemental et militaire courant dans des pays du Groupe des cinq correspondant au critère coté C3.

	3. Analyse des renseignements sur les cybermenaces; 4. Registres de détection et d'évaluation des activités suspectes; 5. Exécution en temps quasi réel de la prévention de menaces et de la réponse à celles-ci et prise de mesures d'atténuation appropriées; 6. Sources de données sur les cybermenaces et les analyses provenant de plusieurs sources; 7. Renseignements sur les menaces; 8. Incident de cybersécurité intégré, analyse des données et alertes de sécurité; 9. Traitement des données structurées et non structurées liées à la cybersécurité.			

Tous les autres termes et conditions restent inchangés.

Tableau des questions et réponses de l'ISQ

Questions et réponses dans la modification 002		
No.	**Question**	**Réponse**
1	Réf. 1.2.3 Portée du processus d'approvisionnement prévu : « Le Canada a l'intention d'adopter une approche itérative et graduelle pour la mise en œuvre. » Est-ce que cela sous-entend que le Canada adoptera une approche d'élaboration et de gestion de projet pour mettre en œuvre la CD-DAR (dans la même approche que celle utilisée pour le C2 réseau CICS) plutôt que d'acheter des outils de sécurité commerciaux, gouvernementaux ou militaires sur étagère comme solution complète?	Pour le projet CD-DAR, l'objectif est de demander des solutions commerciales, gouvernementales ou militaires sur étagère pour la conception et la livraison de la capacité. La ou les solutions seront intégrées au moyen d'une approche itérative et graduelle par un Intégrateur principal dans une solution entière et complète pour le projet de CD-DAR.
2	Le Canada prévoit-il que le MDN agisse à titre d'intégrateur des solutions CD-DAR obtenues sous contrat ou l'industrie sera-t-elle tenue de les intégrer au CORFC?	L'intégration de la capacité de CD-DAR au sein du MDN/FAC sera réalisée par l'Intégrateur principal, en coordination avec l'équipe de gestion de projet ou sous la direction de celle-ci.
3	Réf. Annexe A, Tableau 1 – 01 – « Groupe des cinq (Gp5) ». Fait-on référence à un client militaire ou gouvernemental des États-Unis, du Royaume-Uni, de l'Australie, de la Nouvelle-Zélande ou du Canada ou le projet peut-il concerner une entité non gouvernementale au sein de ces pays du Gp5?	Le « Groupe des cinq » ne désigne pas forcément un client militaire ou gouvernemental, mais tout client en Australie, au Canada, en Nouvelle-Zélande, au Royaume-Uni ou aux États-Unis, de sorte que le projet en question peut concerner une entité non gouvernementale au sein de l'un des pays du Gp5.
4	Le gouvernement publiera-t-il les documents au format Word pour faciliter la transcription des réponses?	Le Canada ne publiera pas les documents dans MS Word. Les fournisseurs sont invités à utiliser les fonctionnalités du logiciel PDF pour convertir les documents en texte modifiable.
Questions et réponses dans la modification 003		
5	Réf. Annexe A, Tableau 1 et 2. Le Canada peut-il préciser que les références de projet avec des solutions commerciales dans l'environnement commercial sont acceptables comme références pour CD-DAR?	Le Canada acceptera les références de projets avec des solutions commerciales dans l'environnement commercial des pays du Gp5.
6	Le Canada peut-il répondre à une recommandation visant à élargir la portée des références de projet pour inclure les pays de l'OTAN ainsi que les pays du Gp5?	Le Canada ne considérera que les références couvrant l'expérience au sein des pays du Gp5.
7	Nous aimerions connaître les partenaires potentiels que nous devrions approcher avec notre solution. Est-il possible de fournir les noms des intégrateurs ou des revendeurs qui ont soumissionné lors de la phase initiale de ce processus? Le Canada a-t-il une liste d'intégrateurs privilégiés qui pourrait être fournie?	Comme il s'agit de la première phase du marché du CD-DAR, SPAC n'a actuellement aucune liste de fournisseurs intéressés ni de liste d'intégrateurs privilégiés à fournir. La présente ISQ permettra de créer une liste des fournisseurs qualifiés. Les fournisseurs qui recherchent des possibilités de partenariat sont invités à s'identifier et à inscrire leur nom sur la liste des fournisseurs intéressés (LIF) liée à l'affichage de l'ISQ sur le site achatsetventes. Les instructions pour s'inscrire sur la liste sont fournies sur le

		côté droit de la page, sous le titre « Identifiez les fournisseurs intéressés par cet avis ».
Questions et réponses dans la modification 004		
8	Le Canada peut-il clarifier le but de la DDR actuellement publiée sur le CD-DAR n ° W6369-20CY06 / B?	Le DDR W6369-20CY06/B ne demande actuellement aucune réponse de fournisseur. Cette DDR restera ouverte après la clôture de l'ISQ et sera utilisée pour informer continuellement l'industrie du processus d'approvisionnement du CD-DAR.
9	Le Canada a mentionné que la Politique des RIT s'appliquera au projet Cyberdéfense – Analyse des décisions et réponse. Le Canada peut-il fournir des informations sur les modalités et conditions potentielles liées à la Politique des RIT en ce moment?	La Politique des retombées industrielles et technologiques (RIT) s'appliquera au projet Cyberdéfense –Analyse des Décision et Réponse (CD DAR). À l'heure actuelle, les modalités des RIT sont fournies à titre informatif seulement et pourraient être modifiées. Ces modalités constituent le fondement de toute exigence en matière de RIT dans un futur contrat CD DAR. Les exigences en matière de RIT pour le projet CD DAR seront élaborées avec tous les fournisseurs qualifiés ultérieurs, en conjonction avec le processus d'engagement relatif aux invitations à se qualifier (IQ). Toute exigence définitive en matière de RIT propre au projet CD DAR sera saisie dans une demande de proposition pour le projet CD DAR. Des renseignements sur la Politique des RIT, y compris la proposition de valeur, se trouvent à l'adresse http://www.canada.ca/rit.
Questions et réponses dans la modification 005		
No.	**Question**	**Réponse**
10	Dans le but de protéger la Couronne et l'approvisionnement, nous souhaitons savoir si la référence à une « association » dans la définition d'« entité » au point 2.2.2 de la section 2.2 sur la terminologie commune renvoie bel et bien au terme défini « association d'entités ». « Entité » signifie un particulier, une compagnie constituée en personne morale, un partenariat, une société, une coentreprise, un syndicat, une association, une fiducie ou toute autre forme d'entité juridique (point 2.2.2 de la section 2.2 sur la terminologie commune). Une association d'entités désigne des entités juridiques distinctes au sein d'un réseau de services professionnels officiellement organisé dont tous les membres fonctionnent en utilisant une image de marque commune. L'accès à la propriété intellectuelle et aux ressources de talent doit être partagé, et la	Le point 3.4 de l'ISQ explique comment l'expérience d'une équipe principale du répondant sera évaluée pour les besoins de l'ISQ. Les « associations d'entités » peuvent soumettre une réponse à l'ISQ. Toutefois, à moins qu'une telle réponse soit soumise comme coentreprise, un membre de l'équipe devra agir comme principal répondant. Les autres membres de l'« association d'entités » devront être soumis comme « membres de l'équipe principale ».

	technologie, la méthodologie, les stratégies et les politiques doivent être intégrées à l'échelle du réseau. Il ne comprend pas les filiales non connexes du répondant avec qui celui-ci collabore en partenariat par l'intermédiaire de l'équipe du répondant ou d'une coentreprise selon le cas (point 2.2.1 de la section 2.2 sur la terminologie commune). Nous espérons que l'intention du Canada était de référer aux « associations d'entités », comme indiqué au point 2.2.1 de la section 2.2 sur la terminologie commune, car cela permettrait de garantir que les entreprises avec des qualifications globales au sein des nations du Groupe des cinq (Gp5), agissant comme des entités juridiques distinctes dans un réseau de services professionnels officiellement organisé, puissent utiliser des projets pour justifier les critères obligatoires et cotés qui n'ont pas été livrés au Canada. Cette modification serait bénéfique pour nous, mais également pour l'ensemble de l'industrie, puisque cela donnerait aux répondants l'occasion de tirer parti d'un plus grand éventail de qualifications globales à partir de leur réseau d'entreprises dans les nations du Gp5. De plus, le Canada est avantagé par la mise en place d'un processus plus compétitif qui comprend une expérience globale des entreprises agissant à titre d'associations d'entités dans leurs réponses à l'invitation à se qualifier (ISQ), fournissant de ce fait au Canada le meilleur aperçu des qualifications et de l'expérience des répondants. Nous ne croyons pas que le Canada avait l'intention d'être inutilement restrictif, mais qu'il visait plutôt à inclure « association d'entités » à même la définition d'« entité ». Puisque le terme « association » n'est pas dans la liste des définitions dans la section 2.2 sur la terminologie commune et que le terme « association d'entités » est défini dans cette même section, mais qu'elle n'apparaît nulle part ailleurs dans l'ISQ, nous pensons que la définition d'« association d'entités » était comprise dans celle d'« entité ». Le Canada pourrait-il confirmer, en publiant une version révisée de l'ISQ, qu'une association d'entités se qualifie comme étant une entité?	
11	La Couronne peut-elle confirmer qu'une référence de projet est acceptable pour justifier les critères obligatoires et cotés pour lesquels le répondant agissait à la fois comme client et fournisseur?	Une référence de projet pour justifier les critères obligatoires et cotés pour lesquels le répondant agissait à la fois comme client et comme fournisseur n'est pas acceptable.
12	Dans le but d'aider la Couronne à évaluer l'expérience et la capacité des répondants à concevoir, élaborer, intégrer, mettre en œuvre et livrer des solutions intégrées antérieures de cybersécurité et d'analyse des décisions et	La personne-ressource du client pour le projet référencé peut résider en dehors des nations du Gp5, mais, comme le mentionnent les critères obligatoires et cotés, le projet doit avoir été réalisé au sein d'une nation du

	réponse, la Couronne peut-elle confirmer qu'une référence de projet est acceptable pour justifier les critères obligatoires et cotés lorsque le lieu du travail effectué est situé au sein des nations du Gp5, mais que le contact client réside à l'extérieur de celles-ci?	Gp5 et pour un client de ce groupe. Les répondants intéressés doivent vérifier les exigences en matière de sécurité énoncées dans la section 1.2 Exigences relatives à la sécurité pour la phase 3 – Diligence raisonnable pour la phase 4 – Demande de propositions et la section 1.3 Exigences relatives à la sécurité pour la phase 5 – Contrat. Ces exigences en matière de sécurité comprennent la limitation, à différents degrés, du brouillon de la demande de propositions et du contrat aux citoyens du Canada, des États Unis, du Royaume Uni, de l'Australie et de la Nouvelle Zélande.
13	Réf. : Tableaux 1 (p. 30) et 2 (p. 33) de l'annexe A. L'État pourrait-il confirmer que des projets de référence mis en œuvre avec succès dans l'IRSC satisfont aux diverses exigences où il est précisé « pour des réseaux de GI-TI complexes composés d'au moins 8 000 points terminaux » au sein d'au moins une des nations du Gp5?	Pour le moment, nous ne pouvons confirmer la conformité du projet de référence réalisé dans l'IRSC. Dans sa soumission, le répondant doit démontrer hors de tout doute que son projet a été réalisé dans une portion suffisamment importante du réseau pour satisfaire à l'exigence des 8 000 nœuds.
14	Conformément à l'annexe B sur les exigences relatives à la sécurité: La compagnie A (États Unis) respecte individuellement l'ensemble des exigences relatives à la sécurité. La compagnie B (Canada) respecte plusieurs exigences de sécurité, mais pas toutes. La compagnie C'est l'entité juridique qui possède à la fois la compagnie A et la compagnie B. Dans ces circonstances, le Canada juge-t-il acceptable, pour les besoins de cette ISQ, que la compagnie C soit identifiée comme principal répondant et que les autorisations de sécurité des compagnies qu'elle possède soient reconnues dans la détermination de sa conformité à l'annexe B sur les exigences relatives à la sécurité?	Les répondants n'ont pas à satisfaire aux exigences relatives à la sécurité des prochaines phases de l'approvisionnement pour répondre à cette ISQ. Les autorisations requises peuvent être obtenues après le processus de l'ISQ. Pour les phases suivantes de l'approvisionnement, toute entité juridique participant au processus doit elle-même détenir les autorisations de sécurité nécessaires afin d'accéder aux renseignements classifiés et pour que l'entité juridique puisse se voir attribuer un contrat. Les autorisations de sécurité d'entités juridiques distinctes ne peuvent être jumelées pour satisfaire aux exigences.
15	Nous aimerions répondre à l'ISQ, mais, à l'heure actuelle, nous ne satisfaisons pas aux exigences relatives à la sécurité de la demande de propositions ou des phases du contrat. Services publics et Approvisionnement Canada ou le ministère de la Défense nationale pourraient-ils financer notre entreprise dans l'obtention des autorisations de sécurité requises?	Le Canada aidera seulement les fournisseurs qui se sont qualifiés à cette ISQ dans l'obtention des autorisations de sécurité nécessaires à la prochaine phase de l'approvisionnement.
16	Dans son invitation à soumissionner, l'État demande ce qui suit : « le renseignement de sources ouvertes (OSINT) pour l'analyse multisources et multiconditions[…]; mener des collectes de renseignements rapides et régulières; mener des activités de déception ». Renseignement externe sur les menaces – Le MDN et les FAC devraient utiliser des flux de type quantitatif proactif, dont l'analyse du Web caché. Le système doit incorporer les flux de service cybernétique de renseignement de sources ouvertes (OSINT) durable, ajustable et de bonne réputation. On comprend ainsi que le soumissionnaire doit démontrer qu'il est en mesure de produire des renseignements liés aux cybermenaces en temps opportun et	L'expérience dans la production des renseignements sur les cybermenaces et connaissance des attaques de l'adversaire ennemi ne sont pas limitées au MDN.

	de proposer au MDN des produits exploitables adaptés aux besoins du Ministère. Il doit également démontrer qu'il connaît l'ennemi et, en particulier, les attaques et les compromissions visant le MDN.	
17	Références sur le rendement antérieur : dans chacun des critères obligatoires du tableau 1 (Critères d'évaluation techniques obligatoires) et chacun des critères d'évaluation cotés du tableau 2 (Critères d'évaluation techniques cotés) de son invitation à soumissionner, l'État demande au fournisseur une référence où il a réalisé avec succès des travaux similaires en précisant les caractéristiques du réseau (p. ex., les points terminaux). De tels détails sont souvent considérés de nature très délicate et même classifiés au sein du Gp5 parce qu'ils révèlent la portée et l'étendue de l'infrastructure du réseau et des opérations qui s'y déroulent. En conséquence, bien que nous souhaitions répondre à l'invitation, nous prévoyons d'importantes difficultés à convaincre nos clients membres du Gp5 d'autoriser la divulgation de renseignements de cette nature. Le MDN et les FAC pourraient-ils envisager de présenter par les voies appropriées des demandes officielles aux agences partenaires homologues au sein du Gp5 dont les capacités de divulgation (à leur discrétion) du portrait et des capacités de leur fournisseur actuel sont comparables?	Dans le cadre de leur invitation à soumissionner, le MDN et les FAC n'envisagent pas de demander aux partenaires du Gp5 de fournir une liste de fournisseurs en mesure de satisfaire aux exigences du projet Cyberdéfence – Analyse des décisions et réponse (CD-DAR). L'État demande au répondant de consulter la section 2, Expérience au sein de projets classifiés, de l'annexe A, Critères d'évaluation obligatoires, de l'invitation à soumissionner. On y décrit la procédure pour établir que l'expérience a été acquise dans le cadre d'un projet classifié et la façon dont l'équipe chargée de l'évaluation, y compris l'autorité contractante possédant la cote sécurité nécessaire, procéderont à l'évaluation du travail réalisé que précise les critères.
18	Nous avons relevé que les références des pays membres de l'OTAN étaient incluses dans l'ébauche de l'invitation à soumissionner, mais absentes de sa version publiée. Le MDN et les FAC peuvent-ils nous faire part des motifs du retrait de ces références?	À la suite d'une analyse plus poussée et dans la foulée de plusieurs consultations menées auprès de divers intervenants, le MDN a décidé de ne pas exiger que le répondant fournisse le nom de pays membres de l'OTAN en référence, puisque cela ne répond pas aux besoins du Ministère.
19	Le MDN et les FAC accepteraient-ils les références des gouvernements d'autres pays que ceux du Gp5 ou des pays membres de l'OTAN?	Les références aux gouvernements qui ne font pas partie du Gp5 ne seront pas prises en compte, puisqu'elles ne satisfont pas aux exigences de l'invitation à soumissionner.
20	Atténuer les risques inhérents au programme par la réduction de la complexité : le projet CD-DAR nécessitera un amalgame de solutions bien intégré provenant de multiples fournisseurs, comme il est indiqué à la section 4.3 de l'énoncé des besoins. Pour accroître la capacité à gérer une solution complète et complexe comme le projet CD DAR, nous suggérons à l'État de réduire le nombre des composantes à intégrer de chaque fournisseur. S'il scinde le projet en portions de moindre envergure, il sera possible de répondre aux besoins liés à celles-ci au moyen de solutions intégrées bien conçues présentant un moindre risque de non-livraison. Selon nous, il importe que le Canada tienne compte du degré élevé de complexité de l'intégration et du déploiement d'un amalgame de	Le nombre de solutions amalgamées ne sera pas pris en compte dans les critères d'évaluation cotés. Les points seront alloués selon le barème appliqué aux critères cotés décrits dans le tableau 2 de l'annexe A.

	solutions, puisque les risques de retard et de défaillance sont directement proportionnels au nombre des composantes. Le MDN et les FAC tiendront-ils également compte du nombre de solutions amalgamées dans les critères d'évaluation cotés?	
Questions et réponses dans la modification 006		
No.	**Question**	**Réponse**
21	Veuillez confirmer que l'exigence « au sein des/pour les pays du Groupe des cinq », englobe les projets déployés dans des entités commerciales et gouvernementales, à l'exception des R4, qui nécessitent un déploiement dans un environnement militaire.	« Pays du Groupe des cinq » ne fait pas référence à un client militaire ou gouvernemental, mais à tout client de l'Australie, du Canada, de la Nouvelle-Zélande, du Royaume-Uni ou des États-Unis, de sorte que les références de projet peuvent provenir d'un déploiement dans une entité non gouvernementale au sein de l'un des pays du Groupe des cinq. Les R4 ne nécessitent toutefois un déploiement que dans un environnement militaire.
22	L'ISQ stipule ce qui suit : « La chasse aux cybermenaces consiste à rechercher de façon proactive et itérative à travers les réseaux pour détecter et isoler les menaces qui échappent aux solutions de sécurité existantes et établissent la persistance dans les réseaux. Il est obligatoire d'être en mesure de surveiller et de contrôler son cyberespace afin qu'il demeure défendable et qu'il chasse les menaces persistantes avancées (MPA). Également : Le système doit fournir les caractéristiques et les données pour appuyer la chasse aux menaces persistantes avancées (MPA), aux menaces intérieures et aux indicateurs. La chasse aux menaces doit donner aux cyberexploitants les moyens de rechercher de façon proactive les activités malveillantes ou anormales qui n'ont pas encore été décelées par les outils de sécurité automatisés du MDN et des FAC, et les analystes de la chasse doivent être formés offensivement. » La chasse aux menaces, les menaces persistantes avancées (MPA) et les cyberopérations offensives sont définies dans la doctrine. Nous suggérons que les FAC demandent une preuve explicite que le soumissionnaire possède ces capacités telles que définies par la doctrine militaire interarmées et que des points sont accordés à ceux qui ont de l'expérience dans la prestation de services aux organismes militaires, de sécurité et de renseignement du Groupe des cinq et en particulier au MDN et aux FAC.	La chasse aux menaces n'est pas propre aux organismes militaires et gouvernementaux. Afin d'encourager la concurrence de différents secteurs de l'industrie ayant de l'expérience en cybersécurité, l'ISQ vise à encourager les soumissionnaires extérieurs aux organismes militaires et gouvernementaux à participer à l'ISQ et à accumuler des points en fonction de leur expérience en matière de capacités de cyberdéfense dans d'autres secteurs.
23	Il y a une exigence énoncée pour la « chasse aux menaces et la découverte de vulnérabilité s'appliquant à l'intelligence artificielle ». Nous suggérons d'attribuer des points cotés à ceux qui utilisent l'IA dans les systèmes de chasse aux menaces livrés au MDN et aux FAC.	Comme il est indiqué au tableau 2 de l'annexe A, les points cotés sont attribués aux entreprises qui ont de l'expérience dans l'utilisation de l'IA dans de multiples domaines de la cybersécurité.

24	L'ISQ demande « le projet CD-DAR avec protection de DDoS cherchera à fournir la possibilité de répudier le trafic malveillant ciblé sur une entité ». Étant donné que la protection DDoS ne peut être mise en œuvre qu'au niveau d'un fournisseur de transporteur s'utilisant de la sécurité et du renseignement en amont. Les FAC ont-elles l'intention que les soumissionnaires signent des ententes de partenariat avec les fournisseurs de télécommunications des FAC?	Les ententes de partenariat avec les fournisseurs de télécommunications du MDN et des FAC ne sont pas requises pour l'ISQ.
25	L'ISQ exige « la capacité d'attribuer les menaces persistantes avancées et d'évaluer les actions, les motifs et les intentions potentiels d'un adversaire opérant sur les réseaux de circonscription ». Nous en déduirons que seuls les soumissionnaires qui ont démontré avec succès l'attribution des MPA contre les FAC/MDN recevraient tous les points cotés.	Les points seront attribués conformément aux critères de notation du tableau 2 de l'annexe A. L'expérience des FAC et du MDN n'est pas requise pour recevoir des points complets pour des critères cotés donnés.
26	L'ISQ exige que les soumissionnaires aient pratiqué « la cyberdéfense active (CDA) en temps réel, c'est-à-dire le processus de participation active et engagée du personnel à la détermination des menaces et à la lutte contre les menaces qui pèsent sur les systèmes ». La cyberdéfense active et les cyberopérations actives sont définies explicitement dans la doctrine des FAC et la loi, comme suit : « mener des activités dans l'infrastructure mondiale de l'information ou au moyen de celle-ci afin de réduire, d'interrompre, d'influencer ou de contrecarrer les capacités, les intentions ou les activités de tout étranger ou État, organisme ou groupe terroriste étranger, dans la mesure où ces capacités, ces intentions ou ces activités se rapportent aux affaires internationales, à la défense ou à la sécurité, ou afin d'intervenir dans le déroulement de telles intentions ou activités ». Les FAC ont-elles l'intention que les soumissionnaires démontrent cette capacité opérationnelle et ces opérations?	Les soumissionnaires doivent démontrer qu'ils ont l'expérience requise pour satisfaire aux critères obligatoires et cotés précisés à l'annexe A.
27	L'ISQ exige la capacité de « mener des activités de déception ». Le Centre de la sécurité des télécommunications (CST) a fourni des conseils en matière de cybersécurité aux ministères sur la question de la cyberdéception, de la dissimulation et de désorientation. La cyberdéception est obligatoire en vertu de l'ITSG-33. Quelles sont les activités de cyberdéception exigées par les FAC?	L'énoncé des besoins opérationnels (EBO) fourni avec l'ISQ contient de l'information sur la conduite des activités de cyberdéception.

28	L'évaluation et autorisation de sécurité (EAS) est le processus par lequel les ministères s'assurent que seuls les logiciels et matériels autorisés sont installés dans leur environnement de technologie de l'information (TI). Le CD-DAR sera-t-il assujetti à tous les contrôles de sécurité en vertu de l'ITSG-33?	Le CD-DAR sera soumis à toutes les exigences d'EAS, y compris les contrôles de sécurité en vertu de l'ITSG-33.
29	Des points seront-ils attribués aux soumissionnaires qui ont déployé avec succès des environnements Protégé B et des environnements infonuagiques classifiés pour le Canada?	Les points seront attribués conformément aux critères de notation précisés au tableau 2 de l'annexe A. Les points d'extrémité ne comprendront que les postes de travail pour ordinateurs portables et de bureau. Les systèmes mobiles ne seront pas inclus.
30	L'ISQ exige ce qui suit : « Le système doit fournir une capacité de détection et d'intervention des points d'extrémités (DIPE) pour déterminer l'installation de logiciels malveillants sous forme de MPA sur un point d'extrémité. » Cela inclut-il les systèmes mobiles? La totalité des points sera-t-elle attribuée aux soumissionnaires qui ont démontré qu'ils ont détecté des MPA aux points d'extrémité des FAC et du MDN?	Les points seront attribués conformément aux critères de notation précisés au tableau 2 de l'annexe A. Les points d'extrémité ne comprendront que les postes de travail pour ordinateurs portables et de bureau. Les systèmes mobiles ne seront pas inclus.
31	Comment la demande de propositions (DP) exigera t elle que les entrepreneurs principaux investissent dans des capacités industrielles clés (CIC) comme la cyberrésilience et l'intelligence artificielle?	La proposition de valeur (PV) et les mécanismes de notation pour l'évaluation des soumissions sont conçus de façon à offrir un cadre souple et sont ajustés en fonction de chaque approvisionnement. Le Canada envisagera des mesures d'incitation à la notation concurrentielle dans les cas où il existe des possibilités d'obtenir des retombées importantes pour les Canadiens. Par exemple, le Canada pourrait utiliser des multiplicateurs de points dans l'évaluation des PV des soumissions pour inciter les soumissionnaires à s'engager à investir dans des capacités industrielles clés (CIC) particulières. À l'heure actuelle, le Canada est en train de déterminer la meilleure approche pour tirer parti des activités économiques liées aux CIC pertinentes dans le cadre de cet approvisionnement. Une analyse préliminaire a ciblé la cyberrésilience et l'intelligence artificielle comme des CIC applicables au projet de CD DAR. Le Canada déterminera comment tirer parti des CIC pertinentes à l'aide de la PV pour le projet de CD DAR en fonction de l'engagement de fournisseurs qualifiés, ainsi que de l'engagement de l'industrie au sens large, des études et analyses de marché et des commentaires d'autres intervenants. À ce titre, à la suite du processus d'évaluation de l'ISQ, le Canada poursuivra son engagement auprès des fournisseurs qualifiés pour le projet de CD DAR afin d'établir toute exigence en matière de retombées économiques.

32	Comment incitera t on les entrepreneurs principaux à établir des partenariats avec les petites et moyennes entreprises (PME) canadiennes?	Les petites et moyennes entreprises (PME) sont d'importantes sources de nouveaux emplois au Canada, et leur participation aux chaînes de valeur mondiales peut se traduire par un important potentiel de croissance. À ce titre, la Politique des RIT exige des soumissionnaires qu'ils s'engagent à entreprendre des activités commerciales au Canada avec des PME canadiennes, généralement à hauteur d'au moins 15 % de la valeur du contrat. Au cas par cas, le Canada s'appuie sur des analyses de marché pertinentes et sur les commentaires de l'industrie avant la demande de propositions finale pour déterminer l'exigence appropriée en matière de PME pour l'approvisionnement en question, et il peut ajuster les exigences dans la demande de propositions finale en conséquence. En outre, le Canada envisagera des incitations à la notation concurrentielle dans les cas où il existe des possibilités d'obtenir des retombées importantes pour les PME canadiennes
33	Veuillez fournir plus d'explications sur ce que les FAC exigent en ce qui a trait à une image commune de la situation opérationnelle (iCSO) au-delà de la définition du glossaire.	À l'heure actuelle, nous ne sommes pas en mesure d'expliquer plus en détail les exigences autres que celles qui ont déjà été fournies dans l'ISQ.
34	Veuillez expliquer plus en détail les exigences en matière de cyberexpertise judiciaire. .	À l'heure actuelle, nous ne sommes pas en mesure d'expliquer plus en détail les exigences autres que celles qui ont déjà été fournies dans l'ISQ.
35	Le CD-DAR sera-t-il intégré à la formation avancée des cyberexploitants dans le cadre du programme IDEeS?	Il est possible que la formation CD-DAR puisse être intégrée à tous les aspects de la cyberformation du MDN et des FAC, y compris la formation avancée des cyberexploitants.
36	L'ISQ stipule ce qui suit : « Capacité de simulation de menaces opérationnelles, de pénétration et d'attaques pour exercer les plages d'essai cybernétique. Il s'agit d'une reproduction de l'ensemble des systèmes d'exploitation avec des jeux de données hors ligne permettant une gamme complète de fonctionnalités et l'exécution de scénarios réalistes à des fins de formation. La solution doit fournir une capacité de simulation de formation pour soutenir la formation opérationnelle collective dans un contexte opérationnel personnalisable. » Le CD-DAR tirera-t-il parti des plages d'essais cybernétiques actuelles? Comment le CD-DAR assurera-t-il l'injection de TTP réalistes de la part des acteurs actuels de la menace? On peut présumer que les soumissionnaires auraient besoin d'une compréhension opérationnelle approfondie des MPA actuelles contre les FAC.	Le CD-DAR tirera parti des plages d'essais actuelles. Une compréhension opérationnelle approfondie des MPA contre les FAC n'est pas requise pour être admissible à l'ISQ.

37	L'ISQ a rendu publique une quantité importante d'information, y compris les exigences opérationnelles et techniques, l'ORBAT, le CONOPS et les lacunes en matière de capacités. Y aura-t-il un plan de sécurité opérationnelle pour les étapes subséquentes du processus?	Les étapes subséquentes de la DP auront des mesures de sécurité supplémentaires qui lui seront appliquées, comme il est indiqué dans la Liste de vérification des exigences relatives à la sécurité (LVERS).
38	L'ISQ n'a pas discuté de la sécurité de la chaîne d'approvisionnement. La sécurité de la chaîne d'approvisionnement sera-t-elle une exigence?	La sécurité de la chaîne d'approvisionnement sera une exigence pour les étapes futures de la DP.
39	Spécifications du point d'extrémité : compte tenu de la portée souhaitée pour le déploiement dans l'ensemble du réseau de commandement du MDN et des FAC, en commençant par le réseau de commandement et le RED, le nombre de points d'extrémité précisés dans chaque série à partir du tableau 1 (Critères d'évaluation technique obligatoires) et du numéro d'exigence du tableau 2 (Critères d'évaluation technique évalués en points) semble assez faible. • Le MDN et les FAC croient-ils que ces exigences sont représentatives de l'ampleur totale du projet? • Ou ces exigences sont-elles considérées comme le point de départ de référence?	Le nombre de points d'extrémité désactivés précisés dans les critères d'évaluation de l'ISQ a été choisi afin d'équilibrer la participation de l'industrie aux exigences du MDN.
40	Formats de données : le critère obligatoire O3 met l'accent sur la capacité d'analyser et de normaliser les formats. Notre expérience avec des projets de même nature est que la normalisation du format de données n'est pas le principal défi. L'échelle des données est le facteur le plus difficile sur le plan technique que le MDN et les FAC devraient envisager d'intégrer à l'ISQ. • Le MDN et les FAC ont-ils envisagé d'inclure des critères de qualification qui mettent l'accent sur la capacité d'une solution de traiter et de gérer les données à une échelle de données précise?	Les critères de gestion des données à l'échelle sont déjà intégrés dans les critères obligatoires.
41	Des outils spécialisés seront toujours nécessaires; l'interopérabilité est primordiale : comme le MDN et les FAC le savent et l'ont décrit dans le CONOPS, le paysage des cyberacteurs malveillants est en constante évolution. Les outils d'aujourd'hui ne suffiraient peut-être plus demain. Il est dans l'intérêt du MDN et des FAC que le CD-DAR soit en mesure d'accepter de nouvelles solutions et d'accepter de nouveaux outils et de maintenir sa capacité d'appuyer la mission dans l'avenir.	1) L'interopérabilité n'est pas une exigence de l'ISQ, mais pourrait être une exigence ou une condition de la DP et du contrat qui en résulte. 2) Il est raisonnable de supposer que la solution finale devra être une combinaison d'outils et de systèmes fournis par les fournisseurs qui sont intégrés aux outils et aux systèmes existants du MDN et des FAC..

	1) L'interopérabilité est l'une des conditions préalables les plus importantes de tout projet de grande envergure couronné de succès, comme le montre l'EOHN no 6 de l'Énoncé des exigences. Nous croyons que c'est la seule façon de garantir que les investissements en TI à grande échelle sont à l'épreuve du temps, d'empêcher le verrouillage des fournisseurs et de s'intégrer avec succès au paysage existant de nos clients. Nous suggérons donc que l'interopérabilité avec les systèmes existants ou futurs soit incluse comme exigence dans l'ISQ. 2) Le CONOPS mentionne plusieurs outils/systèmes (p. ex. GIES, renseignements sur les menaces, gestion des cas). S'attend-on à ce que ces outils/systèmes soient livrés par le fournisseur sélectionné dans le cadre de la solution, ou la solution proposée devra-t-elle interagir/s'intégrer à ces outils/systèmes existants?	
42	Considérations relatives au changement organisationnel : La mise en œuvre du CD-DAR nécessitera une gestion importante du changement organisationnel dans l'ensemble du CEMD. À la section 2.5.2 du CONOPS, le MDN et les FAC ont déjà défini une liste exhaustive des rôles et responsabilités bien définis qui sont nécessaires pour s'attaquer aux cyberactivités existantes dont ils sont responsables. La transition de la multitude actuelle de systèmes disparates qui nécessitent une utilisation manuelle à une solution plus efficace et consolidée dans le cadre du CD-DAR nécessitera une mise à jour des rôles et responsabilités existants (et possiblement introduits) ainsi qu'une mise à jour des processus/procédures existants (introduction de nouveaux) processus/procédures. De plus, à mesure que le paysage des cybermenaces évoluera, le CD-DAR aura besoin de la souplesse nécessaire pour s'adapter aux menaces exigeantes dans un vaste paysage d'organisation complexe du CEMD. Par conséquent, il faudra des préparatifs importants pour former le personnel, élaborer de nouveaux processus et procédures et, probablement, introduire de nouveaux rôles avec de nouvelles responsabilités. • Le MDN et les FAC sont-ils disposés à transmettre et capables de transmettre la façon dont ils prévoient aborder et, en fin de compte, mettre en œuvre le processus de gestion du changement; ces connaissances influenceront les partenaires que nous choisissons dans le cadre de notre réponse? (p. ex. les partenaires les mieux outillés pour aider à la gestion du changement organisationnel qui sera nécessairement planifiée conjointement avec la mise en œuvre technique)	À cette étape du projet, le MDN n'est pas en mesure de transmettre son plan de gestion du changement pour le CD-DAR.

43	Renvoi vers l'invitation à se qualifier (ISQ) – 3.6 Modifications à l'équipe de base du répondant L'État pourrait-il confirmer que, comme il est indiqué aux sous-sections 3.6.1 et 3.6.2 de l'ISQ, les répondants doivent garder la même équipe de base tout au long du processus d'approvisionnement et qu'ils ne sont pas autorisés à ajouter ou à retirer des membres de leur équipe une fois qu'ils se seront préqualifiés dans le cadre de la présente ISQ?	Conformément aux sections 3.6.1 et 3.6.2 de la présente ISQ, aucune modification ne pourra être apportée aux membres de l'équipe de base d'un répondant tout au long du processus d'approvisionnement, ce qui comprend l'attribution et la mise en œuvre du contrat, sauf si la modification est approuvée par écrit par l'autorité contractante. Des modifications à la composition de l'équipe de base pourraient, à la discrétion du Canada, entraîner l'inadmissibilité du répondant dans le cadre du processus d'approvisionnement relatif au projet de CD-DAR.
44	Renvoi vers l'annexe A : Critères d'évaluation obligatoires, pages 28 à 41 Bien que nous comprenions le fait que l'État aimerait mener des vérifications des références pour confirmer la conformité des répondants aux critères d'évaluation de l'ISQ, en raison de la nature confidentielle et classifiée des projets qui répondent à ces critères, les clients de la défense et d'autres clients gouvernementaux n'acceptent pas que leurs coordonnées soient transmises à cette étape du processus d'approvisionnement. Dans la plupart des cas, une approbation est requise à un échelon élevé de l'organisation de défense pour pouvoir citer l'organisation en tant que telle ou un nom, ce qui est une pratique courante pour les organisations de défense nationale. Ainsi, cette exigence relative aux renseignements sur un client cité en référence restreindra de façon considérable, voire éliminera, le nombre de projets du Groupe des cinq (Gp5) que les répondants peuvent citer. Par conséquent, cela réduira de façon artificielle le bassin d'organisations hautement qualifiées et expérimentées qui seront en mesure de se qualifier dans le cadre du présent processus. Nous ne croyons pas qu'il s'agisse de l'intention de l'État, car cela aura une incidence négative sur la capacité du MDN/FAC d'atteindre ses objectifs dans le cadre de ce marché crucial. Donc, le Canada pourrait-il confirmer que si les coordonnées du client cité en référence ne sont pas fournies dans la réponse du répondant à l'ISQ, le répondant disposera de cinq semaines ouvrables pour obtenir les approbations requises afin de transmettre ces renseignements à l'étape d'attribution et de négociation de la DP officielle? Cette option sera avantageuse pour l'État et lui donnerait l'assurance nécessaire avant la signature d'un éventuel contrat.	Comme il est indiqué dans la modification no 006 à la présente ISQ, le Canada acceptera, pour tous les projets, la réception des coordonnées des clients après la date de clôture de l'ISQ, jusqu'à la publication de la DP finale. Toutefois, les répondants ne seront pas considérés comme préqualifiés tant et aussi longtemps que les coordonnées du client n'auront pas été fournies et que l'expérience du projet cité en référence n'aura pas été confirmée par le Canada. Les fournisseurs qui ne sont pas préqualifiés ne pourront pas participer à des activités offertes aux fournisseurs préqualifiés, y compris la réception de la DP finale.
45	Nous travaillons à l'élaboration d'une réponse à l'ISQ pour le projet de CD-DAR. Nous avons remarqué que la date de clôture dans la plus récente modification a été changée pour le 1er décembre 2021. Pourriez-vous confirmer que la	Seule la date de clôture de la DDR a été modifiée au 1er décembre 2021. La DDR no W6369-20-CY06/B est publiée à l'adresse suivante :

	réponse à l'ISQ et aux critères obligatoires est également remise au 1er décembre 2021?	https://achatsetventes.gc.ca/donnees-sur-l-approvisionnement/appels-d-offres/PW-QE-049-27832. Comme il est indiqué sur la principale page d'affichage de cette DDR, même si la DDR est ouverte, elle n'est pas active en ce moment. L'invitation à se qualifier (ISQ) se trouve sur le site Achats et ventes, sous l'avis de projet de marché (APM) no W6369-20-CY06/C, à l'adresse suivante : https://achatsetventes.gc.ca/donnees-sur-l-approvisionnement/appels-d-offres/PW-QE-049-28197. Tous les fournisseurs qui aimeraient se qualifier dans le cadre du projet de CD-DAR doivent soumettre une réponse à cette ISQ.
46	Nous aimerions entamer le processus d'obtention d'une cote de sécurité d'organisation dans le but d'être admissible à soumissionner l'éventuelle DP. Veuillez nous informer des étapes à suivre pour obtenir les cotes de sécurité requises.	Le Canada aidera seulement les fournisseurs qui se sont qualifiés à cette ISQ dans l'obtention des autorisations de sécurité nécessaires à la prochaine phase de l'approvisionnement. Nous rappelons aux répondants intéressés qu'ils doivent examiner les exigences de sécurité dans la section 1.2 Exigences de sécurité pour la phase 3 - Diligence raisonnable, la phase 4 - DP et la section 1.3 Exigences de sécurité pour la phase 5 - Contrat. Ces exigences de sécurité comprennent la limitation, à des degrés divers, du projet de demande de propositions/demande de devis et du contrat aux citoyens du Canada, des États-Unis, du Royaume-Uni, de l'Australie ou de la Nouvelle-Zélande. Des informations sur le processus d'enquête de sécurité de l'organisation sont disponibles à l'adresse suivante : https://www.tpsgc-pwgsc.gc.ca/esc-src/organisation-organization/index-fra.html
Questions et réponses dans la modification 007		
No.	**Question**	**Réponse**
47	Approche progressive et expérimentale : Telle que décrite, l'approche de CD-DAR est détaillée et complète. Cependant, le déploiement des capacités du projet ne produira pas de résultats avant environ trois ou quatre ans et la valeur ne sera pas concrétisée avant ce laps de temps. Une seule année équivaut à une vie entière dans le cyberespace. Les capacités de CD-DAR, comme examinées et définies au cours du processus d'approvisionnement traditionnel, ne seront peut-être plus pertinentes au moment de la mise en œuvre du projet. Durant toute cette période, le ministère de la Défense nationale (MDN) et les Forces armées canadiennes (FAC) n'auront pas profité d'avantages en temps réel.	1. CD-DAR a l'intention d'adopter une approche agile de la conception et la mise en œuvre du système. 2. CD-DAR a l'intention de mettre en œuvre une approche progressive et expérimentale de la modernisation des capacités de cyberdéfense du MDN et des FAC.

	1. Le MDN et les FAC ont-ils envisagé une approche plus agile à la conception et la mise en œuvre du système, comprenant une mise en œuvre expérimentale pour continuer à éclairer le processus en cours tout au long de cette période? 2. Le MDN et les FAC ont-ils envisagé une approche plus progressive et expérimentale de la modernisation de la posture de cyberdéfense, afin de commencer à s'attaquer aux difficultés auxquelles l'organisation cybernétique est confrontée aujourd'hui (p. ex., lancer des projets pilotes pour renforcer les capacités et tester la capacité à s'améliorer)?	
48	À l'annexe A, paragraphe 3, table 1 (intitulée « Critères d'évaluation technique obligatoires ») du document plusieurs des critères obligatoires relatifs à la mise en œuvre avec succès stipulent que les solutions de cybersécurité et d'analyse des décisions et réponses doivent avoir été déployées au sein d'un « environnement réseau de GI-TI complexe d'au moins 8 000 points terminaux ». Au Tableau 2 (intitulé « Critères d'évaluation techniques cotés »), on précise que des points seront accordés en fonction du nombre de dispositifs terminaux du projet, même si ce nombre est inférieur à 8 000. Or ce chiffre est défini comme un critère obligatoire dans la table 1. Le Canada est-il d'avis que les soumissionnaires se verront accorder des points selon le nombre de dispositifs terminaux, qui doivent se situer entre 2 001 et 8 000 dispositifs?	Les points seront accordés conformément aux critères de pointage défini au tableau 2 de l'annexe A. En ce qui concerne les critères obligatoires, on exige au moins 8 000 dispositifs terminaux.
49	Clarification du terme « année-personne » (ISQ, amendement 001, p. 27, annexe A, paragraphe 1.3 (Projets), article 1.3.4 (h)) Étant donné qu'une année-personne peut être définie et calculée de différentes manières, l'État pourrait-il fournir sa propre définition afin de s'assurer que tous les répondants donnent une réponse conforme?	Une année-personne correspond au nombre total de ressources en personnel ayant travaillé à un projet à temps plein au cours d'une année. Par exemple, si une équipe de cinq personnes a travaillé à un projet à temps plein pendant une année, le nombre d'années-personnes serait de cinq (5).
50	Définition du terme « resynchronisation » (ISQ, amendement 001, C1) L'État pourrait-il définir le terme « resynchronisation » utilisé dans le critère C1?	La resynchronisation est définie comme étant la capacité d'un système dans un domaine de prendre automatiquement des mesures pour retrouver un état de sécurité conforme au reste du réseau lorsque le domaine, compte tenu de sa configuration de sécurité approuvée (telle qu'elle est définie dans la base de référence de l'organisation) et de l'état de préparation du système, se désynchronise en raison d'environnements à bande passante déconnectée, intermittente ou limitée (DIL). La resynchronisation comprend également le stockage de l'intégralité des registres et des données intermédiaires de cybersécurité générés localement ainsi que leur transmission en temps quasi

		réel au réseau de base, au fur et à mesure que la connectivité/largeur de bande devient disponible. La resynchronisation doit être effectuée de manière à ce que l'état de sécurité du réseau et de l'hôte soit préservé, que la vulnérabilité soit réduite au maximum et que l'organisation soit protégée contre les menaces tant externes qu'internes avant que la connectivité ne soit perdue.
51	Clarification du terme « preuve d'acceptation » (ISQ, amendement 001, p. 41, Table 3 – Définitions, « Mis en œuvre avec succès ») L'État pourrait-il décrire ce qu'il entend par le terme « preuve d'acceptation » (en considérant que les clients donnent déjà des références et que leurs projets servent de référence)?	Une preuve d'acceptation peut-être un document signé par le client qui reconnaît officiellement que le projet cité en référence a bien été terminé, que toutes les exigences ont été satisfaites et que de l'aide à la stabilisation a été fournie. Comme le stipule la définition, une lettre de soutien d'un client (fédéral) est jugée acceptable. Les clients cités comme référence seront contactés pour vérifier et confirmer l'information fournie par le répondant au sujet du projet cité en référence.
52	Annexe A, paragraphe 1.3 « Projets », article 1.3.1 « Dans le cas où le répondant doit inclure une description de projets : (i) le projet doit avoir été réalisé par le répondant lui-même : l'expérience acquise par un sous-traitant proposé ou une société affiliée au répondant qui ne fait pas partie de l'équipe de base ne compte pas; (ii) un projet doit avoir été mis en œuvre avec succès au cours des sept (7) dernières années suivant la date de clôture de l'ISQ; (iii) plus d'un (1) projet de référence peut être utilisé pour satisfaire à tous les critères d'évaluation, toutefois, pas plus d'un (1) projet de référence ne peut être utilisé pour satisfaire à un critère d'évaluation individuel ». Cela signifie-t-il, par exemple, qu'un fournisseur ne peut pas utiliser un projet A (portant sur 2 000 points terminaux) et un projet B (portant sur 6 000 points terminaux) pour atteindre le critère obligatoire de 8 000 points terminaux? Ou bien cela devrait-il être interprété en présumant que l'État n'évaluera que le premier projet cité en référence, peu importe si d'autres projets sont cités en référence pour le même critère obligatoire? Cette dernière interprétation est souvent appliquée aux contrats de services professionnels conclus avec SPAC.	Le fournisseur ne peut pas combiner des projets pour atteindre le nombre minimal de points terminaux. Conformément à l'article 1.3.1 (iii) du paragraphe 1.3 « Projets », plus d'un (1) projet de référence peut être utilisé pour satisfaire à tous les critères d'évaluation, toutefois, pas plus d'un (1) projet de référence ne peut être utilisé pour satisfaire à un critère d'évaluation individuel. En outre, l'article 1.3.3 du paragraphe 1.3 « Projets » stipule que « Les répondants devraient seulement fournir les projets cités en référence demandés, comme indiqué dans chaque exigence obligatoire. Si le nombre de projets cités en référence est supérieur au nombre demandé, les répondants devront préciser les projets cités en référence qui s'appliquent aux exigences obligatoires ou cotées correspondantes. »
Questions et réponses dans la modification 008		
No.	**Question**	**Réponse**
53	La priorité sera-t-elle accordée aux soumissionnaires canadiens ?	L'ISQ est ouvert à tous les fournisseurs capables de répondre aux critères d'évaluation.

54	La question et la réponse 10 (modification 005) semblent créer un conflit dans la définition d'« association d'entités » et de « membre de l'équipe de base ». La section 2.2.1 indique clairement que l'« association d'entités » constitue des entités liées qui excluent mutuellement les affiliés non apparentés. De plus, la définition d'« association d'entités » précise que le terme « ne comprend pas les affiliés non apparentés au répondant avec qui celui-ci collabore en partenariat par l'intermédiaire de l'équipe de base du répondant ou d'une coentreprise (selon le cas). » La section 2.2.1 n'exige pas que l'« association d'entités » soit nommée comme membres de l'équipe de base ou comme coentreprise. Veuillez confirmer que la section 2.2.1 conserve les exigences initialement communiquées à l'industrie. Notre interprétation d'« association d'entités » était que toute référence de l'entreprise X compterait dans l'ensemble comme relevant du répondant principal et que si on utilisait une référence de n'importe quel autre affilié vaguement conforme, on devrait l'ajouter comme membre de l'équipe de base.	Le terme "association d'entités" a été inclus dans l'ISQ par erreur et n'est pas utilisé dans l'ISQ sauf comme définition à la section 2.2.1. Pour éviter toute confusion, l'ISQ a été modifiée pour enlever ce terme. Conformément à la section 3.3.3 de l'ISQ et la sous-section 1.3.1(i) de l'annexe A, le répondant principal qui inclut l'expérience de projet d'une autre entité doit aussi inclure cette entité comme membre de l'équipe de base dans sa réponse.
55	Nous comprenons qu'aucune attestation de marchandises contrôlées n'est requise avant répondre à l'ISQ. Je comprends que nous devons en disposer d'une avant de recevoir la demande de propositions (DP). D'ici quelle date environ devrons-nous fournir les attestations de marchandises contrôlées pour pouvoir recevoir la DP?	Nous ne sommes pas en mesure de fournir une date pour la diffusion de la DP à l'heure actuelle. Toutefois, les délais généraux du processus d'approvisionnement se trouvent à la section 1.3 – Résumé du processus d'approvisionnement prévu, de l'ISQ.
56	Équipe de base du répondant – Suivi de la question 43, issue de la modification no 006. Nous comprenons que le retrait d'un membre de l'équipe principale que le répondant a utilisé pour se qualifier dans le cadre du présent marché ne serait pas idéal ou avantageux pour l'État. Toutefois, à mesure que les répondants en apprennent davantage sur le projet CD-DAR dans le cadre des rencontres individuelles et du processus de diligence raisonnable, les répondants pourraient découvrir un besoin d'améliorer leur équipe de base en y ajoutant un nouveau membre en vue de s'assurer que le MDN et les FAC obtiennent le meilleur rapport qualité-prix et la meilleure expertise possible. Veuillez confirmer que les répondants peuvent ajouter des membres à leur équipe de base après s'être qualifiés dans le cadre de l'ISQ.	Comme il est indiqué dans la question 43 issue de la modification no 006, pour tous les répondants qualifiés, toute demande de modification aux membres d'une équipe de base d'un répondant, y compris une demande visant à ajouter des membres à l'équipe de base, sera examinée au moment de la demande pour déterminer si la modification proposée est acceptable en fonction des modalités de l'ISQ et de la demande de propositions.
57	Association d'entités – Suivi de la question 10, issue de la modification no 005 Bien que nous sommes reconnaissants du fait que l'État a inclus une définition d'association d'entités dans la DP, le lien entre l'association d'entités et le	La définition de répondant qui figure à la section 2.2 de l'ISQ ne comprend pas les affiliés des répondants et le Canada n'entend pas modifier cette

	répondant semble être manquant. L'État pourrait-il clarifier ce qui suit: 1. Que le répondant comprend les affiliés du répondant; 2. Que les affiliés du répondant comprennent les membres des associations d'entités.	définition. L'ISQ a été modifiée de façon à supprimer l'« association d'entités » de la section 2.2.
58	Pour des raisons de sécurité, nous demandons que le répondant puisse être identifié comme le premier point de contact dans le formulaire 2 pour assurer la liaison avec le client et établir le contact entre le Canada et le client, aux fins de la vérification de la conformité aux critères.	Le répondant pourrait être identifié comme le premier point de contact dans le formulaire 2. Veuillez noter, tel qu'il est indiqué dans la modification no 006 à la présente demande de soumissions et en réponse à la question 44, bien que le Canada accepte les coordonnées du client après la date de clôture de l'invitation à se qualifier et jusqu'à la diffusion de la DP finale, les répondants ne seront pas considérés comme présélectionnés tant que les coordonnées du client ne seront pas fournies et que l'expérience du projet cité en référence n'aura pas été confirmée par le Canada. Les fournisseurs qui ne sont pas pré-qualifiés ne pourront participer à aucune activité ouverte aux fournisseurs pré-qualifiés, y compris la réception de la DP finale.
Questions et réponses dans la modification 009		
No.	**Question**	**Réponse**
59	En ce qui a trait à l'article (c) du critère C3 (ISQ, amendement 001, p. 36, C3), est-ce que l'État pourrait clarifier si les répondants doivent fournir en référence un (1) projet qui satisfait à chacune des exigences (a), (b) et (c) du critère C3? Dans ce cas, nous recommandons fortement à l'État de retirer l'exigence (c), car cela signifie que le répondant doit fournir un projet de référence qui satisfait non seulement au critère C3, mais également aux critères d'évaluation technique obligatoires 1 à 6. Cette méthode est trop restrictive à l'étape de l'ISQ, car selon la structure actuelle du critère C3, les répondants qui satisfont aux critères O1 à O6 et aux exigences (a) et (b) du critère C3 obtiendraient au final une note de 0/20.	Critère C3 modifié comme suit : Le répondant a réussi la mise en œuvre, au cours des sept (7) dernières années, d'un (1) projet de GI/TI complexe comprenant la conception, le développement, l'intégration, la mise en œuvre de solutions commerciales, gouvernementales ou militaires standard intégrées de cybersécurité et d'analyse de décisions et de réponse cybernétique et de resynchronisation dans des pays du Groupe des cinq et de services de soutien à la stabilisation pendant au moins douze (12) mois pour tous les aspects suivants d'un réseau donné : (a) réseau distribué à l'échelle mondiale sur au moins deux (2) continents comportant au moins dix (10) nœuds opérationnels distincts, (b) interconnecté à distance à faible vitesse (liaisons de moins de 1,544 Mbps) dans des environnements austères à un réseau central à haute vitesse (100 Mbps ou plus), et (c) pour la transmission de données liées à la cybersécurité, un réseau de : i) de 2 001 à 4 000 dispositifs terminaux; ii) de 4 001 à 6 000 dispositifs terminaux; iii) de 6 001 à 8 000 dispositifs terminaux;

		iv) Plus de 8 000 dispositifs terminaux Pour le critère C3 (c), le projet du répondant doit inclure au moins cinq (5) des neuf (9) exemples de données et de renseignements liés à la cybersécurité ci-dessous : 1. Identification et suivi des actifs de GI/TI autorisés et non autorisés; 2. Renseignements relatifs à chacune des évaluations des vulnérabilités, de la configuration, des risques et de la conformité aux correctifs; 3. Analyse des renseignements sur les cybermenaces; 4. Registres de détection et d'évaluation des activités suspectes; 5. Exécution en temps quasi réel de la prévention de menaces et de la réponse à celles-ci et prise de mesures d'atténuation appropriées; 6. Sources de données sur les cybermenaces et les analyses provenant de plusieurs sources; 7. Renseignements sur les menaces; 8. Incident de cybersécurité intégré, analyse des données et alertes de sécurité; 9. Traitement des données structurées et non structurées liées à la cybersécurité.