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

LETTER OF INTEREST
LETTRE D'INTÉRÊT

Title - Sujet
Infrastructure de technologie de l'

Solicitation No. - N° de l'invitation	Date
W8474-18IT01/A	2018-05-30
Client Reference No. - N° de référence du client	**GETS Ref. No. - N° de réf. de SEAG**
W8474-18IT01	PW-$$QE-450-26842
File No. - N° de dossier	**CCC No./N° CCC - FMS No./N° VME**
450qe.W8474-18IT01	

Solicitation Closes - L'invitation prend fin
at - à 02:00 PM
on - le 2018-07-17

Time Zone
Fuseau horaire
Eastern Daylight Saving Time EDT

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

Address Enquiries to: - Adresser toutes questions à:	Buyer Id - Id de l'acheteur
Guilderson, Greg	450qe
Telephone No. - N° de téléphone	**FAX No. - N° de FAX**
(819) 956-0564 ( )	( ) -

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

DEPARTMENT OF NATIONAL DEFENCE
2 Constellation Drive
OTTAWA
Ontario
K2G 5J9
Canada

Comments - Commentaires

Instructions: See Herein

Instructions: Voir aux présentes

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

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**

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

Canada

Item Article	Description	Dest. Code Dest.	Inv. Code Fact.	Qty Qté	U. of I. U. de D.	Unit Price/Prix unitaire FOB/FAM Destination	Plant/Usine	Delivery Req. Livraison Req.	Del. Offered Liv. offerte
1	Information Technology Infrastructu	W8474	W8474	1	Each	$	$	See Herein	

Infrastructure de technologie de l'information à l'appui du commandement et du contrôle

-

Lettre d'intérêt

TABLE DES MATIÈRES

OBJET ET CONTENU DE LA PRÉSENTE LETTRE D'INTÉRÊT

La présente lettre d'intérêt (LI) porte sur le projet d'infrastructure de technologie de l'information à l'appui du commandement et du contrôle (ITI C2) pour le ministère de la Défense nationale (MDN) et les Forces armées canadiennes (FAC). L'objet de la présente LI est d'orienter et de préparer l'industrie en vue d'éventuelles possibilités d'approvisionnement concernant le projet d'ITI C2 et de recueillir des commentaires et la contribution en ce qui a trait à la portée, aux exigences, au calendrier, aux risques et aux coûts éventuels du projet. Le contenu général de la présente LI comprend :

PARTIE I : Processus relatif à la lettre d'intérêt – Renseignements sur le processus de la LI et la procédure que doit suivre l'industrie pour répondre à la présente LI

PARTIE II : Solution d'ITI C2

PARTIE III : Questions à l'intention de l'industrie – Questions qui visent à obtenir la rétroaction de l'industrie et qui permettront au MDN et aux FAC de définir leurs besoins et leur analyse de rentabilisation

ANNEXE A : Contexte du projet d'ITI C2
ANNEXE B : Environnement de mission et scénarios opérationnels
ANNEXE C : Énoncé préliminaire des exigences
ANNEXE D : Rétroaction de l'industrie
ANNEXE E : Acronymes

PARTIE I : PROCESSUS RELATIF À LA LETTRE D'INTÉRÈT

1. INTRODUCTION

La présente LI porte sur le projet d'ITI C2 du MDN pour le MDN et les FAC. L'objet de la présente LI est d'orienter et de préparer l'industrie en vue d'éventuelles possibilités d'approvisionnement concernant le projet d'ITI C2 et de recueillir des commentaires et la contribution en ce qui a trait à la portée, aux exigences, aux risques et aux coûts éventuels du projet.

Le projet d'ITI C2 en est à la phase précoce d'analyse des options, ce qui signifie que l'analyse de rentabilisation et la justification du projet sont encore en cours d'élaboration. Ainsi, aucune décision sur les concepts, les technologies ou les solutions n'a été prise. L'objectif de la phase d'analyse des options est de s'assurer que les cadres supérieurs du Ministère peuvent prendre une décision éclairée sur la meilleure façon de définir le projet (c.-à-d. mener la phase de définition) et, si cela est jugé approprié, mettre en œuvre le projet afin de réaliser la capacité requise.

L'intention est de mobiliser et de consulter activement l'industrie pendant les phases d'analyse des options et de définition afin d'assurer la réussite du projet. La rétroaction de l'industrie aidera l'équipe de projet du MDN et des FAC à définir ce qui suit :

a. L'énoncé des besoins (EB) d'une manière compréhensible pour l'industrie et pertinente dans le contexte opérationnel du MDN et des FAC, et ainsi contribuer à bien décrire les besoins opérationnels;

b. L'« art du possible » concernant les capacités en matière de technologie de l'information (TI), l'évolution future au sein de l'industrie et la manière dont les grandes entreprises changent pour répondre à leurs besoins informatiques en évolution, ce qui permet de bien définir l'EB, le budget et le calendrier requis pour atteindre les objectifs du projet (du point de vue technologique et industriel / de l'approvisionnement);

c. Les répercussions sur les personnes, les processus et la technologie des diverses solutions proposées ainsi que les changements organisationnels qui seront nécessaires à l'appui de chaque solution conceptuelle;

d. La nature et les sources de coûts du projet, y compris le besoin de tâches liées à la phase de définition, les coûts de la phase de mise en œuvre et le soutien en service (SES) à long terme;

e. La stratégie d'approvisionnement la plus appropriée qui soit acceptable pour l'industrie pour fournir le bon équipement au MDN et aux FAC en temps opportun, obtenir le maximum de l'argent des contribuables, mettre à profit les achats pour créer des emplois et de la croissance, et simplifier les processus d'approvisionnement.

Le MDN et les FAC ne communiqueront pas avec les fournisseurs à la suite de cette LI. L'autorité contractante présentée à la section 2.7 pourrait communiquer avec l'industrie pour obtenir plus de renseignements à propos des réponses. Toute activité future de mobilisation ou d'approvisionnement de l'industrie sera diffusée publiquement.

1.1 Nature de la présente lettre d'intérêt

La présente n'est pas une demande de soumissions. La présente LI ne donnera lieu ni à l'attribution d'un contrat ni à la création d'une quelconque liste de fournisseurs. Les fournisseurs éventuels de biens ou de services décrits dans la présente LI ne doivent pas réserver de stocks ou d'installations ni affecter des ressources en fonction des renseignements présentés dans celle-ci. Par conséquent, qu'un fournisseur éventuel réponde ou non à cette LI ne l'empêchera pas de participer à un processus d'approvisionnement ultérieur.

De plus, la présente LI ne mènera pas nécessairement à l'acquisition des biens et services décrits qui y sont décrits. La présente LI vise simplement à obtenir des commentaires de l'industrie sur les éléments qui y sont présentés.

2. CONSIGNES À SUIVRE POUR RÉPONDRE À LA PRÉSENTE LETTRE D'INTÉRÊT

2.1 Nature et présentation des réponses demandées

On rappelle aux répondants que ce document est une LI et non une demande de propositions (DP). Ainsi, les répondants sont invités à livrer leurs commentaires, leurs préoccupations et leurs recommandations quant à la façon dont les exigences ou les objectifs décrits dans cette LI pourraient être satisfaits. Ils devraient prendre soin d'expliquer toute hypothèse énoncée dans leurs réponses.

Les réponses ne seront pas utilisées à des fins d'évaluation compétitive ou comparative, et par conséquent, elles n'ont pas besoin d'être données dans un format aussi rigide que le seraient les réponses à une DP. Toutefois, pour faciliter l'utilisation et pour maximiser la valeur des réponses, le Canada demande que les répondants suivent le format présenté à la section 2.6.

2.2 Coûts relatifs aux réponses

Le Canada ne remboursera aucuns frais engagés par les organismes pour répondre à la présente LI.

2.3 Traitement des réponses

Utilisation des réponses : Les réponses ne feront pas l'objet d'une évaluation formelle; le gouvernement du Canada pourra utiliser les réponses reçues afin d'élaborer ou de modifier sa stratégie d'approvisionnement. Le Canada procédera à l'examen de toutes les réponses reçues. Le Canada peut, à sa discrétion, examiner des réponses reçues après la date de clôture de la LI.

Équipe d'examen : Une équipe d'examen composée de représentants du MDN et de Services publics et Approvisionnement Canada (SPAC) examinera les réponses. Le Canada se réserve le droit d'embaucher des experts-conseils indépendants ou d'utiliser des ressources du gouvernement du Canada, pour l'examen des réponses, s'il le juge nécessaire. Chaque réponse ne sera pas nécessairement examinée par tous les membres de l'équipe d'examen.

Confidentialité : Les répondants devraient indiquer les parties de leur réponse qu'ils considèrent comme étant exclusives ou confidentielles. Le Canada traitera ces réponses, conformément aux exigences de la *Loi sur l'accès à l'information*.

2.4 Communication avec l'industrie

L'autorité contractante peut communiquer avec l'industrie pour obtenir plus de renseignements à propos d'une réponse.

2.5 Contenu de la lettre d'intérêt

Les renseignements contenus dans le présent document évoluent constamment. C'est pourquoi les répondants ne doivent pas perdre de vue que de nouvelles exigences pourraient être ajoutées à toute demande de soumissions que publiera éventuellement le Canada. Les répondants ne doivent pas non plus supposer qu'aucune des exigences ne sera supprimée ou révisée. Les répondants sont donc invités à faire part de leurs commentaires sur tout aspect des exigences. La présente LI contient également des questions précises adressées à l'industrie.

26 Format de présentation des réponses

Page couverture : si la réponse comprend plusieurs volumes, le répondant doit indiquer, sur la page couverture de chacun des volumes, le titre de la réponse, le numéro de la LI, le numéro du volume ainsi que la dénomination sociale complète du répondant.

Page titre : La première page qui suit la page de couverture doit représenter la page titre. Celle-ci doit comporter les éléments suivants :

i. Le titre de la réponse et le numéro du volume;

ii. Le nom et l'adresse du répondant;

iii. Le nom, l'adresse et le numéro de téléphone du représentant du répondant;

iv. La date;

v. Le numéro de la LI.

Nombre de copies : Le Canada demande que les répondants présentent leur réponse en format PDF [en version 2003 ou plus récente] non protégé (c.-à-d. sans mot de passe). Si la taille du document est inférieure à six mégaoctets (Mo), le Canada demande aux répondants de l'envoyer par courriel à TPSGC.PADivisionQE-APQEDivision.PWGSC@tpsgc-pwgsc.gc.ca. Si la taille du document PDF est égale ou supérieure à 6 Mo, le Canada demande aux répondants d'en enregistrer une copie sur deux clés USB et de les envoyer par la poste à l'agent des contrats dont les coordonnées figurent à la section 2.7.

Les réponses à la présente LI peuvent être rédigées dans l'une ou l'autre des langues officielles du Canada, soit en anglais ou en français.

27 Demandes de renseignements

Toutes les demandes de renseignements et autres communications relatives à la présente LI doivent être présentées uniquement directement à l'autorité contractante de SPAC. Comme il ne s'agit pas d'une demande de soumissions, le Canada ne répondra pas nécessairement par écrit et ne donnera pas forcément de réponses à tous les répondants; toutefois, les répondants qui ont des questions concernant la présente LI peuvent les transmettre à :

Autorité contractante : Greg Guilderson ou Jeff Moore

Services publics et Approvisionnement Canada
Place du Portage III, bureau 8C2
11, rue Laurier
Gatineau (Québec) K1A 0S5
819-956-0564
Adresse courriel : TPSGC.PADivisionQE-APQEDivision.PWGSC@tpsgc-pwgsc.gc.ca

Veuillez inscrire « ITI C2 » sur la ligne objet pour éviter un retard de la réponse.

Le courriel électronique est la méthode préféré de communication.

28 Présentation des réponses

Date et lieu de présentation des réponses : Les organisations souhaitant fournir une réponse doivent la remettre à l'autorité contractante indiquée à la page 1 de la présente LI, au plus tard à la date et à l'heure de clôture indiquées à la page 1 de la présente demande de soumissions.

La date de clôture de la LI n'est pas la date limite pour présenter des commentaires ou des

contributions. Les commentaires et les contributions seront acceptés jusqu'à ce qu'un suivi concernant la demande de soumissions soit publié.

Identification de la réponse : Chaque répondant doit s'assurer que son nom, son adresse et le numéro de la LI figurent lisiblement sur l'enveloppe contenant la réponse.

Renvoi des réponses : Les réponses à la présente LI ne seront pas renvoyées.

29 Surveillant de l'équité

Si un processus d'approvisionnement de solution d'ITI C2 est enclenché, le Canada retiendra les services d'une organisation qui agira à titre de tiers indépendant comme surveillant de l'équité. Le rôle du surveillant de l'équité consistera à fournir une preuve d'assurance en matière d'équité, d'ouverture et de transparence des activités faisant l'objet de surveillance.

Le surveillant de l'équité devra notamment assumer les responsabilités suivantes :

i. Surveiller le processus d'approvisionnement en totalité ou en partie (ce qui comprend notamment les processus liés à l'engagement et à la DP prévue);

ii. Faire part de ses commentaires au Canada sur des questions relatives à l'équité;

iii. Prouver l'équité du processus d'approvisionnement.

Veuillez noter que, dans le but d'exécuter ses obligations liées à la surveillance de l'équité, le surveillant de l'équité aura accès aux réponses de l'industrie et à la correspondance connexe reçue par le Canada à la suite de la présente LI. En outre, le surveillant de l'équité peut, à titre d'observateur, assister aux activités éventuelles de suivi en matière d'engagement et de passation de contrats.

PARTIE II : SOLUTION D'ITI C2

1. CONTEXTE DE LA SOLUTION D'ITI C2

Le MDN et les FAC ont besoin de mettre en place une infrastructure de TI sécurisée et intégrée de niveau secret qui permettra d'assurer la convergence des réseaux secrets du MDN et des FAC et d'en réduire le nombre; de renforcer les capacités en matière de connectivité et d'échange de renseignements au sein du MDN et des FAC ainsi qu'avec nos partenaires de mission; d'évoluer rapidement pour répondre aux futurs défis. Cette infrastructure de technologie de l'information permettra aux commandants des FAC d'exercer le commandement et le contrôle (C2), y compris dans un quartier général déployé, en utilisant les dernières technologies disponibles pour offrir des capacités de soutien optimales.

Le MDN et les FAC fourniront cette nouvelle capacité par l'intermédiaire du projet d'ITI C2, qui s'efforcera, entre autres, de tirer parti des capacités et des efficiences de l'industrie afin d'offrir des services autant que possible.

Le projet d'ITI C2 en est actuellement à la phase d'analyse des options : l'option de mise en œuvre préférée devrait être déterminée et sélectionnée d'ici juin 2019. Cette phase sera suivie d'une phase de définition puis d'une phase de mise en œuvre; la capacité opérationnelle initiale est prévue pour juin 2025 et la capacité opérationnelle totale d'ici septembre 2027.

2. OBJECTIF DE LA PRÉSENTE LI

La présente LI est publiée aux fins suivantes :

a. Consulter l'industrie pour mieux comprendre les possibilités offertes et émergentes en matière d'infrastructure de technologie de l'information commerciale et de solutions de service;
b. Obtenir des renseignements de l'industrie concernant le prix et la disponibilité de l'infrastructure de TI commerciale et des solutions en matière de service.
c. Obtenir des renseignements pour aider le MDN et les FAC à établir leurs besoins et aider au processus interne de planification et d'approbation pouvant mener à une demande de soumissions;
d. Obtenir des renseignements pour aider le MDN et les FAC à regrouper éventuellement certains des produits livrables énumérés à l'annexe C, afin qu'un fournisseur ou une équipe de fournisseurs puisse offrir une solution intégrée pour un sous-ensemble cohérent de produits livrables.

La présente LI ne signifie pas que le Canada a pris une décision définitive quant aux possibilités d'approvisionnement. Le MDN et les FAC peuvent décider de ne choisir aucune des solutions ou aucun équipement indiqués dans les réponses. En aucune circonstance, le Canada ne sera tenu responsable à l'égard d'un fournisseur ayant préparé une réponse à la présente LI.

3. EXIGENCES EN MATIÈRE DE SÉCURITÉ

Aucune exigence relative à la sécurité n'est liée à la présente LI.

Toute mesure d'approvisionnement future prise en appui à la solution d'ITI C2 exigera que les fournisseurs soient inscrits au Programme des marchandises contrôlées; elle pourrait exiger que les fournisseurs détiennent une habilitation de sécurité de niveau II (secret) et éventuellement une habilitation de niveau III (très secret) émise par leur agence de sécurité nationale. Certains des fournisseurs pourraient aussi devoir respecter les exigences du gouvernement du Canada pour fournir des produits et offrir des services assortis de restrictions (classifiées) de type Réservé aux Canadiens.

Pour obtenir plus de renseignements sur le Programme des marchandises contrôlées, cliquez ici :

https://www.tpsgc-pwgsc.gc.ca/pmc-cgp/index-fra.html

4. EXCEPTION AU TITRE DE LA SÉCURITÉ NATIONALE

Afin de protéger les intérêts de sécurité nationale, le Canada invoquera son droit en vertu des accords commerciaux nationaux et internationaux d'utiliser une exception au titre de la sécurité nationale (ESN) dans le cadre du présent processus d'approvisionnement. L'ESN permet au Canada de soustraire un processus d'approvisionnement de certaines ou de l'ensemble des obligations d'un accord commercial visé lorsqu'il le juge nécessaire afin de protéger ses intérêts en matière de sécurité nationale ou des intérêts connexes indiqués dans le texte des ESN.

5. POLITIQUE DES RETOMBÉES INDUSTRIELLES ET TECHNOLOGIQUES (RIT)

Le présent besoin n'est pas assujetti aux accords commerciaux internationaux, mais s'inscrit plutôt dans le cadre de la Stratégie d'approvisionnement en matière de défense annoncée le 5 février 2014. En conséquence, la Politique des RIT accompagnée de la proposition de valeur peut donc être appliquée à ce processus d'approvisionnement. La Politique des RIT est administrée par Innovation, Sciences et Développement économique (ISDE) Canada.

5.1 Application de la Politique des retombées industrielles et technologiques (RIT)

La Politique des retombées industrielles et technologiques (RIT) peut être mise en application dans le cadre du projet de l'infrastructure de technologie de l'information à l'appui du commandement et du contrôle (l'ITI à l'appui du C2). Dans le cadre d'une lettre d'intérêt (LI), la participation de l'industrie aidera à déterminer comment appliquer la Politique des RIT et la façon dont le Canada pourrait tirer profit des avantages économiques grâce à ce processus.

5.2 La Politique des RIT, notamment la proposition de valeur

La Politique des RIT est un outil puissant qui sert à attirer des investissements. Les entreprises qui se voient attribuer des marchés d'approvisionnement en matière de défense sont tenues de mener des activités commerciales au Canada dont la valeur équivaut à celle du marché. La Politique des RIT encourage les entreprises à s'établir au Canada ou à y accroître leur présence, à renforcer leurs chaînes d'approvisionnement au pays ainsi qu'à développer des capacités industrielles canadiennes.

La Politique des RIT vise à soutenir la viabilité à long terme et la croissance du secteur de la défense du Canada, y compris les petites et moyennes entreprises de partout au pays, à stimuler l'innovation au Canada au moyen de la R-D, à appuyer le développement des compétences et la formation, ainsi qu'à accroître le potentiel d'exportation des entreprises établies au Canada. La Politique des RIT comprend une proposition de valeur (PV) qui exige des soumissionnaires qu'ils se fassent concurrence sur la base des retombées économiques pour le Canada associées à chaque soumission. Les soumissionnaires retenus sont sélectionnés en fonction du prix, du mérite technique et de la proposition de valeur. Les engagements relatifs à la PV pris par le soumissionnaire retenu deviennent des obligations contractuelles dans le contrat subséquent.

Pour en savoir plus sur la Politique des RIT, consultez le site www.canada.ca/rit.

5.2.1 Capacités industrielles clés

Dans l'espoir d'optimiser l'impact économique de la PV, le Canada utilisera la Politique des RIT en vue d'encourager les entrepreneurs du secteur de la défense à investir dans les capacités industrielles clés (CIC). Les CIC sont harmonisées avec la politique de défense du Canada, *Protection, sécurité, engagement*, et le *Plan pour l'innovation et les compétences*, elles appuient le perfectionnement des compétences et encouragent l'innovation dans le secteur de la défense du pays. Ces CIC sont liées à des domaines de technologies émergentes qui présentent un potentiel

de croissance rapide et des débouchés importants, à des capacités établies par rapport auxquelles le Canada est concurrentiel à l'échelle mondiale et à des domaines où la capacité nationale est essentielle à la sécurité du pays.

Le gouvernement a déterminé que cet approvisionnement nécessite des capacités dans les domaines de la **cyberrésilience** et de l'**intelligence artificielle**. Ces CIC sont des technologies émergentes et, à ce titre, elles présentent un potentiel de croissance rapide et d'innovation. Pour cette raison, le Canada désire créer de nouveaux débouchés dans ces domaines et, pour ce faire, encouragera les partenariats et les investissements auprès du secteur et d'établissements postsecondaires appuyant le perfectionnement des connaissances, de même que la recherche et le développement.

Voici les définitions des CIC concernées par ce projet :

Cyberrésilience
La cyberrésilience couvre tous les aspects des secteurs de la sécurité nationale, civile et commerciale, et rectifie les vulnérabilités créées par l'expansion de la technologie de l'information et de l'économie du savoir. La cyberrésilience comporte des activités de conception, d'intégration et de mise en œuvre de solutions technologiques qui protègent l'information et les réseaux de communication. Ces technologies, parmi d'autres, doivent être axées sur le développement efficace des cybercapacités suivantes :

Sécurité de l'information
La protection des données et des renseignements électroniques et numériques contre l'accès et toute intrusion, l'utilisation, la divulgation, la perturbation, la modification, la consultation, l'inspection, l'enregistrement ou la destruction non autorisé.

Sécurité informatique
La sécurisation du contenu et la gestion des menaces (point terminal, messagerie, réseaux, Web, nuage), sécurité, gestion des vulnérabilités et des risques, gestion de l'identité et de l'accès, et autres produits (p. ex. des trousses de chiffrement et de gestion des jetons, et des essais de vérification de produits de sécurité), ainsi que des services d'éducation, de formation et de connaissance de la situation.

Sécurité des technologies opérationnelles
La surveillance, mesure et protection des systèmes d'automatisation et de contrôle des processus industriels et connexes. La cyberrésilience peut comprendre la création d'outils et l'intégration de systèmes et de processus qui renforcent la sécurité des systèmes tactiques ou des grands réseaux, le chiffrement, la cyber-expertise et les interventions en cas d'incident, entre autres. Les capacités établies dans ce domaine pourraient s'appuyer de plus en plus sur l'IA à titre de technologie habilitante. Ainsi, des réseaux feraient usage de leurs défenses de façon autonome et dynamique contre les intrusions et se répareraient eux-mêmes après une perturbation.

Intelligence artificielle
L'intelligence artificielle, ou IA, couvre un éventail de technologies qui permettent à des machines de réaliser des tâches qui nécessitent habituellement l'intelligence humaine, telles que la reconnaissance des formes et de la parole, la traduction, la perception visuelle et la prise de décisions. L'IA s'appuie sur diverses disciplines, comme les algorithmes de recherche et l'optimisation mathématique, l'apprentissage machine, l'apprentissage approfondi, l'autoapprentissage et les réseaux neuronaux, en plus d'étendre les connaissances qui s'y rattachent. Elle allège la charge de travail des utilisateurs et automatise les tâches facilement répétables où ils doivent intervenir. L'IA permet d'envisager un meilleur rendement du personnel formé, de soustraire celui-ci à des

environnements dangereux et de s'adapter plus rapidement aux changements dans l'environnement opérationnel militaire. Elle simplifie également de nombreuses activités, telles que l'analyse de quantités massives de données à l'appui du renseignement, de la planification des missions, de l'entraînement connexe, de la logistique, de la gestion opérationnelle, de la cybersécurité et de la cyberrésilience. L'intelligence artificielle a sa place dans de nombreux domaines liés à la défense et d'autres secteurs.

6. LANGUES OFFICIELLES

Tout marché futur visant une solution d'ITI C2 pourrait exiger que l'entrepreneur fournisse tous les documents ainsi que le soutien technique et le soutien aux clients dans les deux langues officielles.

7. APPROCHE EN MATIÈRE D'ENGAGEMENT

7.1 Mobilisation de l'industrie

Le processus de mobilisation de l'industrie commence avec la présente LI et prendra fin au moment où une demande de renseignements officielle, une DP ou un autre processus concurrentiel sera envoyé aux fournisseurs.

La présente LI est publiée sur https://achatsetventes.gc.ca/ afin de permettre à l'industrie d'échanger des renseignements avec SPAC et le MDN sur la situation actuelle du marché, les technologies disponibles et les capacités des fournisseurs.

Étant donné que le MDN et les FAC en sont à la phase précoce de l'analyse des options du présent processus d'approvisionnement, l'approche de mobilisation de l'industrie au-delà de la présente phase est toujours en cours d'élaboration.

PARTIE III : QUESTIONS À L'INTENTION DE L'INDUSTRIE

1. QUESTIONS À L'INTENTION DE L'INDUSTRIE

1.1 Domaines d'intérêt

1.1.1 Quelles fonctions énumérées à l'annexe A – section 5 (Fonctions et technologies d'intérêt du projet) seriez-vous intéressé à fournir ou à appuyer, et dans quel(s) rôle(s) précis (p. ex., intégrateur de système, fournisseur de dispositifs, installateur du site, vérificateur et valideur, formateur, fournisseur du soutien en service, etc.)?

1.1.2 Y a-t-il d'autres fonctions qui ne sont pas énumérées à l'annexe A – section 5 que vous recommanderiez à l'équipe de projet et que vous seriez intéressé à fournir ou à appuyer et, le cas échéant, dans quel(s) rôle(s) précis (p. ex., intégrateur de système, fournisseur de dispositifs, installateur du site, vérificateur et valideur, formateur, fournisseur du soutien en service, etc.)?

1.2 Expérience

1.2.1 En ce qui concerne les fonctions que vous avez précisées à la section 1.1 :

a. Avez-vous de l'expérience dans la prestation de ces fonctions ou de fonctions semblables pour une infrastructure informatique prenant en charge entre 25 000 et 50 000 utilisateurs, sur des établissements très éloignés géographiquement? Sinon, quelle est la quantité maximale d'utilisateurs de l'infrastructure informatique sur laquelle vous avez travaillé?

b. Avez-vous de l'expérience dans la prestation de ces fonctions ou d'autres fonctions semblables dans un environnement classifié? Sinon, avez-vous de l'expérience dans la prestation d'autres solutions d'infrastructure informatique en environnement classifié?

c. En ce qui a trait aux expériences précitées, veuillez fournir un résumé de votre rôle (p. ex., intégrateur de système, fournisseur de dispositifs, installateur du site, vérificateur et valideur, formateur, fournisseur du soutien en service, etc.), de votre expérience et des exemples de projets ou de contrats (maximum de trois exemples pour chacun, s'il y a lieu) ainsi que le nom et le type de client(s) (industrie privée, organisation gouvernementale).

1.3 Solutions recommandées

1.3.1 Quelle est votre vision d'une ou de plusieurs solutions pour l'année 2025 qui satisferaient à une partie ou à l'ensemble des exigences et des fonctions d'un projet, conformément à l'annexe C — section 2 (Exigences générales et produits livrables)?

1.3.2 Quelles sont vos solutions proposées? Veuillez décrire en termes généraux la manière dont les solutions proposées satisferaient aux exigences précises du projet, y compris leurs avantages et leurs inconvénients, et formuler des recommandations pertinentes, le cas échéant.

1.3.3 Recommanderiez-vous que certains aspects de l'infrastructure informatique soient conçus ou approvisionnés par le MDN et les FAC? Lesquels?

1.3.4 Recommanderiez-vous que le MDN et les FAC mettent en œuvre certains aspects de l'infrastructure informatique dans le cadre de la solution globale? Lesquels?

1.3.5 Quelles fonctions de l'infrastructure informatique recommanderiez-vous de regrouper sous forme de trousse pour la solution fournie?

1.3.6 Quelle stratégie de mise en œuvre recommandez-vous? Une livraison par étapes? Comment passeriez-vous de l'ancien système au nouveau système tout en assurant une exploitation continue?

1.3.7 Y a-t-il des tendances précises dans le domaine des technologies informatiques sur lesquelles vous recommanderiez que le MDN et les FAC explorent parce qu'elles pourraient permettre une meilleure exécution des fonctions énumérées à l'annexe A?

1.3.8 Veuillez fournir le cas échéant les fiches de produit pertinentes pour les produits et les solutions que vous proposez.

1.4 Technologie infonuagique

1.4.1 Dans le contexte d'une solution d'infonuagique pour l'environnement classifié :

a. Quelles seraient vos recommandations, y compris les avantages et les inconvénients, sur l'utilisation d'un nuage public, d'un nuage privé et d'un nuage hybride comme solution complète ou partielle?

b. Seriez-vous en mesure de fournir une infrastructure spécialisée au MDN et aux FAC dans un environnement de nuage public (c.-à-d., nuage privé virtuel)? Dans l'affirmative, veuillez expliquer.

c. S'il y a lieu, veuillez expliquer comment votre solution tirerait automatiquement et dynamiquement profit du nuage public pour appuyer et augmenter un nuage privé du MDN et des FAC dans un environnement hybride.

d. Comment le MDN et les FAC seraient-ils en mesure de surveiller vos solutions et les données appartenant au MDN et aux FAC pour satisfaire à l'exigence de contrôle autoritaire?

e. Comment le MDN et les FAC, en particulier notre centre d'exploitation du réseau et nos administrateurs de système, pourraient-ils accéder à la configuration et à l'état de tout l'équipement informatique et des logiciels?

f. Quelle stratégie recommanderiez-vous pour migrer les données du MDN et des FAC de notre réseau vers votre solution infonuagique?

g. Quelle stratégie de sortie recommanderiez-vous pour migrer les données de votre infrastructure ou de votre solution à l'expiration du contrat?

h. En cas de fuite de données, comment le MDN et les FAC auraient-ils accès à vos sites pour effectuer le nettoyage (c.-à-d., effacer les données et les disques)?

1.5 Gestion de l'identité et des droits d'accès, service de sécurité axé sur les données

1.5.1 En ce qui concerne les fonctions de gestion de l'identité et des droits d'accès (GIDA) énumérées à l'annexe A :

a. Veuillez décrire les types de services que vous fournissez et expliquer le fonctionnement de chacun.

b. Comment votre solution de GIDA fonctionnerait-elle avec une infrastructure à clés publiques (ICP) reposant sur un système d'authentification et de justificatifs d'identité? Quel type de changement d'interface serait nécessaire pour intégrer un système d'ICP existant?

c. Quelle serait l'incidence de votre solution de GIDA sur la configuration et le déploiement d'Active Directory?

d. Comment votre solution de GIDA fonctionnerait-elle avec une liste de contrôle d'accès, un contrôle de l'accès fondé sur les rôles, un contrôle de l'accès fondé sur les attributs et un contrôle de l'accès fondé sur les politiques?

e. Votre solution de GIDA procure-t-elle un accès par justificatifs d'identité à facteurs multiples? Dans l'affirmative, veuillez expliquer.

f. Votre solution fonctionne-t-elle dans un environnement centralisé ou réparti (de 15 à 20 sites environ)? Quels sont les avantages, les inconvénients et les limites d'une solution centralisée ou répartie?

1.5.2 En ce qui concerne le service de sécurité axé sur les données :

a. Quelles sont les classifications de données (Sans classification, Secret, etc.) actuellement approuvées que peut protéger votre solution ou votre produit axé sur les données? Y a-t-il des progrès qui permettraient d'accroître les fonctions actuelles de protection et de classification? Dans l'affirmative, veuillez expliquer.

b. Quelle est votre stratégie de protection de l'information stockée et transmise?

c. Quelles sont les contraintes et les limites de votre service de sécurité axé sur les données?

d. Quelles normes ont été ou sont utilisées dans l'élaboration du service de sécurité axé sur les données (y compris les métadonnées)?

e. Comment votre système interagirait-il avec d'autres domaines sans fonctions semblables ou avec des domaines qui utilisent un service de sécurité axé sur les données différent?

f. Votre système pourrait-il fonctionner avec une solution comme GCDocs?

g. Comment votre système fonctionnerait-il dans un environnement temporairement déconnecté?

h. La méthode de chiffrement utilisée par le système peut-elle être mise à niveau indépendamment du système lui-même?

i. Quelle est la granularité des règles administratives qui peuvent être créées? Peut-on l'adapter à certains ensembles de données?

j. Quelle approche a été adoptée pour vérifier les transactions traitées par le service de sécurité axé sur les données? Est-elle intégrée à la gestion des incidents de sécurité ou s'agit-il d'une application autonome?

k. Quels sont les rôles standard nécessaires pour administrer votre service de sécurité axé sur les données? Le système prend-il en charge la séparation des tâches et les flux de travail souples pour attribuer les rôles administratifs?

l. Votre solution fonctionne-t-elle dans un environnement centralisé ou réparti (de 15 à 20 sites environ)? Quels sont les avantages, les inconvénients et les limites d'une solution centralisée ou répartie?

m. Comment votre solution fonctionnerait-elle avec des données de systèmes anciens? Existe-t-il un outil pour migrer les données de tels systèmes vers le nouvel environnement? Veuillez quantifier l'effort nécessaire pour migrer de telles données (léger, modéré, important, très important) et décrire le processus.

1.6 Facteurs de coûts pour le MDN et les FAC

1.6.1 Quels sont les principaux facteurs de coûts pour le MDN et les FAC d'une solution complète et des éléments individuels?

1.6.2 Quelle est la modélisation des coûts de votre solution, y compris les principales mesures utilisées pour déterminer les coûts? Avez-vous une tarification progressive en fonction du nombre?

1.6.3 Quels renseignements seraient nécessaires pour vous permettre de fournir des estimations de coûts plus substantielles?

1.6.4 Veuillez fournir des estimations de coût selon un ordre de grandeur approximatif (séparé en gestion de projet, services d'ingénierie et durée prévue, coûts du matériel et des logiciels) de votre solution proposée, y compris s'il y a lieu :

a. élaboration des spécifications détaillées du système;

b. élaboration de la conception détaillée du système;

c. création et déploiement d'un environnement d'essai et de développement;

d. le cas échéant, développement et déploiement de prototypes;

e. évaluation et approbation de la sécurité;

f. évaluation des besoins en formation;

g. matériel ou logiciels supplémentaires;

h. autres questions de configuration, d'installation ou de déploiement;

i. services d'ingénierie divers;

j. coûts d'exploitation payés par le MDN et les FAC (y compris le nombre prévu d'employés nécessaires pour appuyer et analyser les données afin de livrer la fonction);

k. coûts du soutien en service et de l'entretien défrayés par le MDN et les FAC.

1.6.5 Dans la mesure du possible, veuillez fournir les coûts selon un ordre de grandeur approximatif d'une solution de soutien en service entièrement externalisée (y compris le nombre prévu de personnes nécessaires pour assurer un soutien 24 heures sur 24 et 7 jours sur 7)?

1.6.6 Quels services de soutien en service annuels fourniriez-vous? Pouvez-vous fournir des estimations des coûts annuels selon un ordre de grandeur approximatif et, le cas échéant, des frais annuels pour les licences et la maintenance?

1.7 Risque

1.7.1 Prévoyez-vous d'autres risques que ceux énumérés au tableau suivant?

Risques techniques	Risques en matière de sécurité	Risques externes	Risques organisationnels	Risques liés à la gestion du projet
• Exigences • Technologie • Innovation • Intégration • Complexité et interfaces • Fonctions • Performance et fiabilité • Qualité	• Employés • Matérielle • Gestion de l'information • Technologie de l'information • Industriel • Contrat	• Opérationnel • Sous-traitants et fournisseurs • Réglementation • Marché • Client • Météo et environnement	• Dépendances du projet • Ressources - Ressources humaines - Financement - Formation - Infrastructures • Établissement des priorités • Services juridiques	• Portée • Calendrier • Estimation • Planification • Contrôle de gestion • Communications

1.7.2 Selon votre expérience, comment quantifieriez-vous chaque risque énoncé, à l'aide d'une échelle Faible, Moyen ou Élevé?

1.7.3 Parmi les fonctions décrites à l'annexe A — section 5, quelles sont les cinq qui, selon vous, présentent le risque le plus élevé d'un point de vue technique? Veuillez les énumérer par ordre de risque décroissant, et justifier brièvement vos choix.

1.8 Contrats

1.8.1 Quelle approche (p. ex., achat, location ou combinaison) recommanderiez-vous pour l'approvisionnement de l'infrastructure informatique et des solutions proposées? Veuillez expliquer.

1.8.2 Quelle approche contractuelle (p. ex., un seul contrat sous un seul contracteur, plusieurs contrats sous un ou plusieurs contracteurs) recommanderiez-vous pour l'approvisionnement de l'infrastructure informatique? Veuillez expliquer.

1.8.3 Quelle durée (y compris les années optionnelles) recommanderiez-vous pour le contrat visant les éléments de l'infrastructure informatique en location? Veuillez expliquer.

1.8.4 Quelles approches en matière de prestation et de passation de marchés recommanderiez-vous pour le soutien en service après le déploiement, y compris la durée et les options? Veuillez expliquer.

1.8.5 Quelles approches en matière de prestation et de passation de marchés recommanderiez-vous pour la formation après le déploiement, y compris la durée et les options? Veuillez expliquer.

1.9 Évaluation

1.9.1 Quelle stratégie en matière d'évaluation technique recommanderiez-vous pour évaluer les propositions de fournisseurs? Veuillez expliquer.

1.10 Questions à l'intention de l'industrie sur la PV et les RIT de l'ITI à l'appui du C2

Secteur de la défense

La Politique des RIT vise à promouvoir le développement économique et la viabilité à long terme des entreprises canadiennes chargées de la fabrication et de la prestation de produits et de services aux fins d'utilisation dans les applications de défense et de sécurité du gouvernement.

1.10.1 En vous fiant aux spécifications techniques énoncées par le ministère de la Défense nationale, décrivez les activités de travail direct que votre société prévoirait entreprendre au Canada pour les CIC énoncées plus haut, relativement à la production et au maintien du projet de l'ITI à l'appui du C2.

Développement des sources d'approvisionnement

La Politique des RIT vise à accroître la compétitivité de l'industrie canadienne en encourageant sa participation ainsi qu'en développant les sociétés nationales, y compris les petites et moyennes entreprises (PME).

1.10.2 La Politique des RIT exige qu'au moins 15 pour cent de l'obligation en matière de RIT de l'entrepreneur (égale à la valeur du contrat) consiste en du travail avec des PME canadiennes de moins de 250 employés. Dans quelle mesure pouvez-vous satisfaire à une telle exigence pour favoriser le développement de PME canadiennes (tant pour ce qui est du travail direct lié à cet approvisionnement qu'au travail mené dans d'autres secteurs d'activités)?

1.10.3 Mis à part l'approvisionnement dont il est ici question, quels autres secteurs de production et de prestation de services présentent selon vous des occasions d'appuyer le développement de PME – qui ont des capacités pertinentes pour les CIC susmentionnées – tout en répondant à la demande nationale et internationale?

Développement des compétences et formation

La Politique des RIT encourage le développement et le maintien d'une main-d'œuvre canadienne talentueuse, novatrice et caractérisée par une forte diversité par l'accès à la formation, à l'enseignement, aux occasions et aux programmes.

1.10.4 Quelles sortes d'investissements dans le développement des compétences et la formation sont selon vous les plus profitables pour le secteur de la défense ou le secteur commercial du Canada?

a. Exemples :
    i. les programmes en milieu de travail (p. ex. stages coop, placements professionnels);
    ii. les programmes d'apprentissage;
    iii. un nouveau programme ou un programme actuel de développement des connaissances d'un établissement postsecondaire (p. ex. codage et programmation, réseautique, développement et intégration de logiciels);
    iv. la prise en charge des attestations de sécurité (p. ex. Très secret, ITAR) et des attestations de conformité à la cybersécurité pour les sociétés canadiennes, en particulier les petites et moyennes entreprises.

Recherche et développement (R-D)

La Politique des RIT encourage la recherche scientifique qui explore le développement de nouveaux biens et services, de nouveaux intrants à la production et de nouvelles méthodes de production des biens et services, ou de nouvelles façons d'exploiter et gérer des organisations.

1.10.5 Existe-t-il des occasions de faire équipe avec des établissements de recherche financés par les fonds publics ou avec des établissements d'enseignement postsecondaire afin d'effectuer des activités de travail direct pour le projet de l'ITI à l'appui du C2?

1.10.6 Pourrait-on créer des consortiums de recherche ou des centres d'excellence en partenariat avec des établissements de recherche financés par les fonds publics ou avec des établissements d'enseignement postsecondaire pour les CIC susmentionnées? Si tel est le cas, dans quels domaines de recherche votre organisation se lancerait-elle?

a. Sinon, quels autres partenariats de recherche ou de développement pourrait-on former en vue d'appuyer le développement technologique pour les CIC susmentionnées?

1.10.7 Est-il possible d'investir dans des partenariats de recherche et de développement avec des PME et des entreprises de démarrage canadiennes, y compris le financement des activités de R-D qui en sont aux dernières étapes et la commercialisation de produits ou de services novateurs?

1.10.8 Quelle devrait être l'exigence minimale de R-D (en pourcentage du prix de l'offre anticipée) afin de motiver les soumissionnaires à investir dans une innovation de grande valeur dans le secteur des CIC du Canada?

Exportation

La Politique des RIT favorise la capacité des entreprises canadiennes, y compris les PME, à exploiter avec succès les marchés d'exportation, augmentant ainsi leur productivité et leur compétitivité sur le marché mondial.

1.10.9 Décrivez les possibilités d'exportation en provenance du Canada directement liées à ce processus d'approvisionnement.

1.10.10 Est-il possible de garantir des droits de propriété intellectuelle suffisants et un mandat de production mondiale exclusif pour exporter dans le cadre de vos opérations canadiennes, y compris les filiales et les partenaires de la chaîne d'approvisionnement?

1.10.11 Veuillez décrire les possibilités d'exportation de grande valeur à partir du Canada concernant des applications de cybersécurité générales, tant dans le secteur commercial que celui de la défense, pouvant être exploitées grâce à cet approvisionnement.

Autres questions

1.10.12 Y a-t-il d'autres CIC pertinentes dans le cadre du travail qui sera mené pour le projet de l'ITI à l'appui du C2? Si oui, indiquez les CIC qui devraient être envisagées et la raison pour laquelle elles devraient l'être. Dans votre réponse, décrivez également la façon dont les CIC proposées accroîtraient les avantages de la proposition de valeur pour l'industrie canadienne.

1.10.13 Comparativement au prix et au mérite technique, la proposition de valeur a généralement une pondération de 10 % de la note globale de la soumission. Que pensez-vous d'une telle pondération pour la proposition de valeur dans le cadre du projet de l'ITI à l'appui du C2?

1.10.14 Dans le cadre de la proposition de valeur, quelle pondération minimale (en pourcentage) recommanderiez-vous d'attribuer aux piliers de la proposition (c.-à-d. le secteur de la défense, le développement des sources d'approvisionnement, les compétences et la formation, la recherche et développement, et les exportations)?

ANNEXE A : CONTEXTE DU PROJET D'ITI C2

1 INTRODUCTION

La présente annexe présente un survol général du projet de l'infrastructure de technologie de l'information à l'appui de commandement et de contrôle (ITI C2) afin que les fournisseurs potentiels puissent estimer et évaluer la portée et le degré de complexité du projet. On demande aux fournisseurs de prendre connaissance de ces renseignements afin de comprendre les facteurs de coûts des solutions et la façon dont les descripteurs quantitatifs décrits ci-dessous peuvent servir à préciser les coûts des solutions propres à chaque spécification ou exigence de performance énoncée à l'annexe C.

Des renseignements plus détaillés seront fournis aux fournisseurs à une étape ultérieure du processus de mobilisation de l'industrie.

2 DESCRIPTION DU PROJET

Le projet de l'infrastructure informatique à l'appui du C2 vise à mettre en place une infrastructure informatique sécurisée et intégrée de niveau Secret afin de réduire le nombre de réseaux cotés Secret du MDN et des FAC ainsi que d'améliorer la connectivité et les fonctions d'échange de données au sein du MDN et des FAC et avec nos partenaires de mission. Cette infrastructure doit permettre une évolution rapide pour relever les défis futurs. Le projet permettra aux commandants de l'ensemble des FAC d'exercer le C2, y compris aux quartiers généraux déployés, au moyen des plus récentes technologies disponibles pour fournir des fonctions optimales de soutien. Pour atteindre ses objectifs, le projet tirera parti dans toute la mesure du possible des fonctions et de l'efficacité de l'industrie dans la prestation des services. Le projet devrait permettre de préciser une option de mise en œuvre privilégiée d'ici à la fin juin 2019, qui sera suivie de l'étape de définition, puis de l'étape de mise en œuvre. La fonction opérationnelle devrait entrer en service initial en juin 2025 et être pleinement en service en septembre 2027.

Le projet de l'infrastructure informatique à l'appui du C2 remaniera et réutilisera les fonctions, les services et la gouvernance de l'infrastructure informatique actuelle de C2 de niveau Secret dans le but de combler les principales lacunes et de répondre à la vision du chef d'état-major de la Défense (CEMD) d'un système intégré d'information de C2 (C2IS). Elle mettra à niveau l'infrastructure informatique Secret de C2, afin de fournir aux utilisateurs des services intégrés sécurisés et en temps opportun à tous les renseignements opérationnels et institutionnels dont ils ont besoin et auxquels ils ont le droit d'accéder, de collaborer avec les organismes gouvernementaux, les alliés et d'autres partenaires, de soutenir les services à fort débit de données, comme la fusion des données et le ciblage, et de permettre une évolution rapide pour relever les défis à venir. Cette mise à niveau reposera sur la mise en place d'une infrastructure informatique cohésive et intégrée de niveau Secret qui réduira le nombre de réseaux disparates et améliorera la connectivité pour faciliter le partage et l'échange de données, de vidéos et d'éléments multimédia ainsi que la téléphonie au sein du MDN et des FAC et avec nos partenaires de mission, et ce, dans tous les domaines de sécurité.

Le projet fournira des fonctions durables de traitement et d'échange d'information pour les systèmes nationaux de C2 de niveau Secret qui relient les organisations du MDN et des FAC dans l'ensemble du pays. Cette connectivité permettra aux commandants de l'ensemble des FAC d'exercer le C2, notamment par la collecte et le traitement d'information provenant d'une grande variété de sources, la planification et la prise de décisions, la direction, la coordination et le contrôle des forces afin d'obtenir un avantage opérationnel sur les adversaires.

De plus, le projet permettra la connectivité à certaines organisations déployées aux niveaux opérationnel et tactique, tant au Canada qu'à l'étranger. Par exemple, il peut s'agir d'un quartier général de la Force opérationnelle interarmées (FOI) des FAC déployé dans le cadre d'une coalition au Moyen-Orient, d'un quartier général de la FOI régionale (FOIR) déployé en Colombie-Britannique pour aider à la suite d'une catastrophe ou d'une frégate déployée dans le cadre de l'opération ARTEMIS dans la mer d'Arabie. Dans

n'importe laquelle de ces missions déployées, un environnement épisodique sera établi pour que le commandant de mission puisse exercer le C2 sur les forces déployées. Ces réseaux déployés seront généralement établis par la FOIR, la nation ou le commandement responsable, et exigent à la fois une connectivité à l'infrastructure informatique de C2 de niveau Secret du MDN et des FAC et une interopérabilité avec d'autres réseaux déployés. L'architecture de ces réseaux déployés sera compatible avec le Réseau canadien des missions déployées (RCMD), le Mission Partner Environment (MPE) des États-Unis et le Future Mission Network (FMN) de l'Organisation du traité de l'Atlantique Nord (OTAN). L'infrastructure informatique à l'appui du projet de C2 fournira la connectivité aux éléments canadiens déployés et aux réseaux connexes déployés pour appuyer les fonctions nationales de C2 du CEMD, du commandant du Commandement des opérations interarmées du Canada (COIC) et des commandants du contingent national canadien. Cette fonction procurera un accès robuste aux services et aux sources d'information documentée hébergés sur les réseaux du MDN et des FAC, du Gouvernement du Canada (GC), des États-Unis (y compris le Commandement de la défense aérospatiale de l'Amérique du Nord (NORAD)), du Groupe des cinq (FVEY) et de l'OTAN, qui peuvent ne pas être accessibles depuis le réseau de la mission. Le projet fournira l'infrastructure informatique pour permettre l'interopérabilité technique et informationnelle et des services fiables, opportuns et sécuritaires d'échange et de traitement de l'information. La connectivité à ces organisations déployées reposera sur une variété de moyens différents, y compris l'internet, les communications par satellite et les systèmes radio stratégiques. (Nota : L'approvisionnement en nouveaux systèmes de communications par satellite et de systèmes radio stratégiques dépasse la portée du présent projet.)

Il est à noter que le projet mettra à profit, dans la mesure du possible, les initiatives d'ingénierie existantes et prévues du MDN et des FAC afin de minimiser tout risque lié à la conception, à la mise en œuvre et à l'intégration de la nouvelle infrastructure informatique de C2 de niveau Secret (p. ex., solutions interdomaines (SID)). Les conceptions et les fonctions développées jusqu'à présent seront mises à la disposition des fournisseurs qui pourront les utiliser selon les besoins.

3 STRATÉGIE DE MISE EN ŒUVRE

L'analyse initiale a établi que le projet devra très probablement reposer sur une approche d'approvisionnement hybride de construction et d'achat pour atteindre ses objectifs. Dans le cadre d'une telle approche hybride, le MDN et les FAC s'associeront à l'industrie pour concevoir, construire, mettre en œuvre et intégrer la nouvelle infrastructure informatique de niveau Secret, tout en conservant le rôle d'intégrateur principal du système ainsi que la possibilité de fournir et de mandater des solutions clés pour une partie de l'infrastructure.

Les particularités en matière d'approvisionnement (p. ex., les exigences relatives aux exceptions en matière de sécurité nationale, les contrats uniques ou multiples, etc.) seront déterminées au fil de l'analyse des diverses options.

4 INFRASTRUCTURE INFORMATIQUE ACTUELLE DE NIVEAU SECRET — DESCRIPTEURS QUANTITATIFS

Les descripteurs quantitatifs suivants donnent un aperçu de l'infrastructure informatique actuelle de niveau Secret du MDN et des FAC, réseaux autonomes compris, et se veulent un point de départ pour l'analyse, sans négliger la croissance et les améliorations prévues dans le cadre du présent projet dans les limites de taille et de capacité propres au MDN et aux FAC :

- Utilisateurs : 15 000
- Applications : 150
- Serveurs : 1 000
- Postes de travail (clients lourds et légers) : 10 000
- Routeurs et commutateurs : 800
- Points de présence (urbains et distants) : 125

- Centres de données nationaux (2) : 60 pétaoctets chacun
- Centres de données déployés (typiquement, de 10 à 15 à tout moment) : 100 téraoctets chacun
- Capacité — sites urbains : 20 mégabits par seconde (Mbit/s)
- Capacité — bureaux : 100 Mbit/s

5 FONCTIONS ET TECHNOLOGIES D'INTÉRÊT DU PROJET

Le projet de l'infrastructure informatique à l'appui du C2 se penchera notamment sur les fonctions et les technologies suivantes, car elles ont le potentiel d'atteindre les objectifs du projet (en notant que l'exploitation en environnement classifié impose des restrictions en matière de sécurité pour l'utilisation de certaines fonctions et technologies) :

a. Infonuagique (y compris prise en charge des périodes de pointe) :

   - nuage public
   - nuage privé
   - nuage hybride
   - technologie de l'information-service (ITaaS)
   - plateforme-service (PaaS)
   - infrastructure-service (IaaS)
   - conteneurs d'application
   - Microsoft Office 365

b. Centres de données :

   - définis par logiciels (virtualisation)
   - centralisés et répartis
   - solutions de stockage
   - solutions de sauvegarde et de récupération
   - solutions d'archivage

c. Active Directory de Microsoft

d. GIDA :

   - service d'identité numérique[1]
   - service de justification d'identité[2]
   - service de gestion des droits d'accès[3]
   - service d'authentification[4]
   - service d'autorisation et d'accès[5]
   - service de cryptographie[6]
   - service de vérification et de rapport[7]

e. Contrôles de l'accès basé sur les attributs et sur les rôles

f. ICP

g. Gestion des droits d'accès numériques et individuels

h. Services de courriel Microsoft Exchange

i. Services de navigation internet

j. Services de clavardage

k. Services de voix par internet (VoIP)

l. Services sécurisés de vidéoconférence (salles de conférence et bureaux)

m. Soutien à la vidéo en temps réel pleine vitesse

n. Protection du système hôte :

- gestion
- pare-feu du système hôte
- contrôle des applications du système hôte
- authentification du système hôte
- vérification de l'intégrité du système hôte
- système de prévention d'intrusions du système hôte
- protection contre les maliciels
- contrôle des ports
- contrôle des périphériques
- chiffrement des supports amovibles
- chiffrement des fichiers et des dossiers
- chiffrement intégral du disque
- vérification des étiquettes de fichiers
- vérification des étiquettes de messages
- effacement à distance
- conformité de la configuration sécurisée
- détection d'un système hôte indésirable

o. Réseautage :

- routage dynamique
- multidiffusion
- réseaux locaux sans fil
- réseaux virtuels
- réseaux définis par logiciels
- virtualisation des fonctions du réseau
- qualité du service (QS)
- surveillance du réseau
- optimisation du réseau
- intégration avec un site à bande étroite (c.-à-d., connecté par satellite)

p. Chiffrement des données classifiées enregistrées au moyen de systèmes gouvernementaux standard ou de systèmes commerciaux (c.-à-d., solutions commerciales pour des systèmes classifiés)

q. Chiffrement des données classifiées pendant leur transfert, au moyen de systèmes gouvernementaux standard ou de systèmes commerciaux (c.-à-d., solutions commerciales pour des systèmes classifiés)

r. Étiquetage des données (c.-à-d., métadonnées et marquage de sécurité des documents jusqu'au niveau du paragraphe)

s. Passerelle d'échange de l'information au sein du domaine Secret (courriel, clavardage, navigation internet, partage de fichiers, téléphonie sur protocole internet (IP), services de vidéoconférence protégée, centraux de services d'annuaire et applications spécialisées)

t. Solutions de transfert interdomaines au sein du domaine Secret et parmi les autres niveaux de sécurité (courriel, clavardage, navigation internet, partage de fichiers, téléphonie sur IP), services de vidéoconférence protégée, centraux de services d'annuaire et applications spécialisées)[8]

u. Système de sécurité multiniveau (p.ex., utilisateur détenant une cote de fiabilité approfondie qui accède à des données de niveau Sans classification sur l'infrastructure de niveau Secret)

v. Appareils des utilisateurs :

- solutions interdomaines d'accès[9]
- client lourd
- client léger (bureaux hôtes virtuels et infrastructure du bureau virtuel)

w. Services de continuité opérationnelle

x. Services de reprise après sinistre

y. Processus de la Bibliothèque d'infrastructure des technologies de l'information (BITI) et outils commerciaux de soutien :

- gestion des biens (matériels et logiciels);
- gestion des configurations
- gestion du changement
- gestion des versions
- etc.

z. Système centralisé de gestion et de surveillance :

- surveillance et gestion du réseau
- surveillance et gestion des centres de données

aa. Soutien logistique intégré (SLI) :

- formation
- soutien en service

Notes :

[1] Identité numérique : représentation de l'identité dans un environnement numérique. Les services d'identité numérique comprennent les processus de saisie et de validation de l'information afin d'identifier une personne de façon unique, d'établir la pertinence et l'adaptation, ainsi que de créer et de gérer une identité numérique tout au long du cycle de vie.

[2] Vérification des justificatifs d'identité : lier une identité à un justificatif physique ou électronique, qui peut par la suite servir de substitut à l'identité ou de preuve de possession d'attributs précis.

[3] Gestion des droits d'accès : l'ensemble des processus permettant d'établir et de maintenir les autorisations ou droits d'accès qui composent le profil d'accès d'une personne, c'est-à-dire les caractéristiques d'une personne qui peuvent tenir lieu de critères pour accorder ou non l'accès à des ressources logiques ou matérielles. Cette fonction permet la gestion des données qui constituent les privilèges de l'utilisateur ainsi que d'autres attributs, y compris l'accès à l'information, son stockage et son organisation.

[4] Authentification : processus de confirmation qu'une identité revendiquée est authentique et repose sur des justificatifs valides. L'authentification conduit généralement à un niveau d'assurance mutuellement partagé par les parties se fiant à l'identité. Elle peut se faire au moyen de divers mécanismes, notamment questions et réponses, séquence de codes synchronisés, comparaison biométrique, ICP ou d'autres techniques.

[5] Autorisation et accès : processus d'octroi ou de refus de demandes spécifiques pour obtenir et utiliser des services de traitement de l'information ou de données et pour accéder à des installations précises. Elles garantissent que les personnes ne peuvent utiliser que les ressources auxquelles elles ont droit, uniquement aux fins approuvées, en assurant l'application des politiques de sécurité qui régissent

l'accès à l'échelle de l'entreprise.

[6] Cryptographie : utilisation et gestion du chiffrement et du déchiffrement afin d'assurer la confidentialité et l'intégrité des données, y compris les fonctions nécessaires comme l'historique des clés et l'entiercement des clés. La cryptographie sert souvent à sécuriser les communications faites par des personnes et des entités impersonnelles.

[7] La vérification et la création de rapports portent sur l'étude des dossiers et des activités afin d'évaluer la pertinence des contrôles du système et la présentation des données enregistrées de façon intelligible.

[8] Les solutions de transfert interdomaines constituent des technologies de haute sécurité qui permettent le transfert de l'information entre les domaines de sécurité, et l'accès à cette information, au moyen d'une inspection robuste du contenu et du contrôle des flux d'information. Les solutions interdomaines présentent le risque le plus faible, et sont approuvées par la National Security Agency (NSA) et le Centre de sécurité des télécommunications (CST). Elles permettent la connexion entre des domaines de sécurité différents.

[9] Les solutions interdomaines d'accès procurent aux utilisateurs un environnement informatique unique pour accéder à plusieurs domaines de sécurité. Par exemple, un utilisateur accédant à deux domaines de sécurité pourrait afficher sur un même écran le réseau étendu de la Défense (RED) et l'infrastructure du réseau secret consolidé (IRSC). L'utilisateur peut passer d'un domaine de sécurité à un autre de la même manière qu'il passe d'une fenêtre d'un navigateur internet à une autre. Chaque domaine reste indépendant, car les données ne peuvent être transférées ni accessibles hors de leur domaine.

6 ÉTAT DU PROJET

Le projet est mené conformément au cadre standard du MDN et en est actuellement à l'étape de l'analyse des options. Cette étape porte sur l'examen et l'évaluation des options générales relevées lors de l'étape précédente de détermination, la réalisation de l'analyse de rentabilisation et la recommandation d'une option privilégiée en vue de la mise en œuvre du projet (l'option privilégiée pourrait être une variante des options actuellement proposées ou même être différente, si les examens de la présente étape, y compris les commentaires de l'industrie et d'autres parties prenantes, le justifient).

Dans le cadre du projet, on a relevé les trois options suivantes pour les soumettre à un examen plus approfondi :

Option 1 — Plus d'un réseau de niveau Secret. Un seul réseau intégré de niveau Secret peut être impossible, vu les solutions technologiques disponibles et les politiques de sécurité, ou il peut présenter des risques inacceptables. Dans cette option, les 25 réseaux classifiés (ou plus) seraient regroupés en une seule infrastructure réseau qui accueillerait plusieurs (mais moins de 25) domaines de sécurité de niveau Secret, c.-à-d. les restrictions et les communautés d'intérêts sensibles, isolés les uns des autres (par des dispositifs informatiques non chiffrés spécialisés et le cas échéant une séparation virtuelle, par exemple). L'utilisateur accéderait aux domaines de sécurité distincts au moyen d'un seul terminal, mais devrait se connecter séparément à chacun d'entre eux. À partir de ce terminal unique, l'utilisateur pourrait après sa connexion afficher les données de plusieurs domaines de niveau Secret simultanément, mais il utiliserait obligatoirement des passerelles d'échange de l'information et des solutions interdomaines automatisées pour transférer l'information entre les domaines de sécurité. Chaque utilisateur aurait besoin d'une cote de sécurité de niveau II (Secret).

Un étiquetage exact et contraignant des données, par l'étiquetage des métadonnées, garantirait l'application des restrictions en matière de classification de sécurité, de diffusion, de manipulation et de communautés d'intérêts. Une fonction de GIDA permettrait à l'utilisateur d'accéder aux réseaux, aux applications et aux services présents sur les divers réseaux. Le soutien du système serait simplifié, car un tel regroupement permettrait une plus grande efficacité et une meilleure sécurité.

Option 2 – **Un seul réseau de niveau Secret.** Avec cette option, les 25 réseaux classifiés ou plus seraient regroupés en une seule infrastructure de réseau prenant en charge un nombre réduit de domaines de sécurité de niveau Secret, c.-à-d., les restrictions et les communautés d'intérêts sensibles. La séparation des domaines de sécurité viserait les données plutôt que le système (p. ex., aucun besoin de dispositifs informatiques non chiffrés ou d'une séparation virtuelle). La séparation des domaines de sécurité et des communautés d'intérêts reposerait sur les justificatifs d'identité de l'utilisateur, les politiques et les restrictions d'accès ainsi que les mécanismes d'autorisation. L'utilisateur aurait un seul terminal, une seule connexion aux multiples domaines de sécurité et à partir de cette connexion unique un accès simultané à toutes les données de niveau Secret pour lesquelles il dispose des droits d'accès, y compris s'il y a lieu le transfert de données entre les domaines de sécurité. Chaque utilisateur aurait une cote de sécurité de niveau II (Secret).

Cette option réduirait considérablement le temps nécessaire pour trouver, obtenir, analyser, traiter et partager l'information opérationnelle et situationnelle critique. Cette fonction améliorée rehausserait beaucoup la capacité des commandants de prendre des décisions et accroîtrait la qualité et la rapidité de l'analyse faite par l'état-major, afin d'avoir un avantage opérationnel sur les adversaires. Un service de sécurité axé sur les données garantirait l'application de la classification, de la diffusion, du traitement et des restrictions de sécurité de manière à contrôler soigneusement l'accès aux données en fonction des autorisations de sécurité et du besoin de savoir de chaque utilisateur. Un système de GIDA permettrait à l'utilisateur d'accéder aux réseaux, aux applications et aux services. Le soutien du système serait simplifié, car il serait plus efficace de gérer et de sécuriser une seule infrastructure réseau de niveau Secret.

Option 3 – **Une infrastructure de réseau de niveau Secret destinée aux utilisateurs détenant une cote Secret et aux utilisateurs sans cote de sécurité.** Avec cette option, les 25 réseaux classifiés ou plus seraient regroupés en une seule infrastructure réseau prenant en charge un nombre réduit de domaines de sécurité de niveau Secret, c.-à-d., les restrictions et les communautés d'intérêts sensibles. La séparation des domaines de sécurité viserait les données plutôt que le système (p. ex., aucun besoin de dispositifs informatiques non chiffrés ou d'une séparation virtuelle). La séparation des domaines de sécurité et des communautés d'intérêts reposerait sur les justificatifs d'identité des utilisateurs, les politiques et les restrictions d'accès ainsi que les mécanismes d'autorisation. L'utilisateur ayant une cote de sécurité de niveau Secret aurait un seul terminal, une seule connexion aux multiples domaines de sécurité et un accès simultané à partir de cette connexion unique à toutes les données de niveau Secret pour lesquelles il dispose des droits d'accès, y compris le cas échéant pour le transfert de données entre les domaines de sécurité. De plus, afin de soutenir les activités de C2 menées sur les applications non classifiées, l'utilisateur sans cote Secret pourrait accéder aux données non classifiées stockées sur l'infrastructure de réseau Secret sans savoir qu'il s'y trouve des données classifiées. Cette option permettrait la migration des fonctions actuelles de soutien du C2 des infrastructures de réseau non classifiées vers les infrastructures de réseau de niveau Secret et faciliterait les processus de C2 répartis sur les deux niveaux de sécurité, sans qu'il soit nécessaire que tous les utilisateurs travaillant au niveau non classifié aient une cote de niveau II (Secret).

Ce système d'accès et de sécurité à niveaux multiples réduirait encore davantage le temps nécessaire à un utilisateur pour trouver, obtenir, analyser, traiter et partager l'information opérationnelle et situationnelle critique (Secret et non classifiée) à partir d'un seul terminal. Cette fonction améliorée rehausserait également la capacité des commandants de prendre des décisions et d'accroître la qualité et la rapidité de l'analyse faite par l'état-major, afin d'avoir un avantage opérationnel sur les adversaires. Elle garantirait également que l'utilisateur non autorisé ne puisse accéder qu'à des renseignements non classifiés résidant sur l'infrastructure de réseau de niveau Secret. Il serait possible de minimiser les améliorations apportées à l'infrastructure en réutilisant l'infrastructure actuelle du RED et les solutions interdomaines. On pourrait migrer les principales activités et fonctions de soutien au C2 non classifiées vers le nouveau système, ce qui améliorerait la sécurité opérationnelle et permettrait de conserver les données sensibles pertinentes au niveau Secret.

7 ANALYSE DES OPTIONS

L'analyse des options sera menée conformément au cadre standard de projet du MDN, plus précisément la Directive sur l'approbation de projet du MDN.

Cette analyse comprend l'évaluation de chaque option viable en fonction des critères cotés suivants :

Description	Mesures connexes ou justification de l'évaluation, selon le cas
Concordance stratégique	Comment chaque option aide-t-elle à atteindre les résultats stratégiques?
Concordance opérationnelle	Comment chaque option aide-t-elle à atteindre les résultats opérationnels souhaités?
Estimation indicative des coûts	Quel est le coût estimatif de la mise en œuvre de chaque option? Quel est le coût total estimatif de la possession, pour la durée de vie du système, de chaque option?
Analyse de rentabilisation	Comment se comparent les coûts et les avantages de chaque option (rapport coût-efficacité, coûts déplacés ou évités)?
Mise en œuvre et capacité	Comment chaque option se compare-t-elle à la capacité du MDN et des FAC (ressources humaines, processus, connaissances, matériaux et infrastructures) de mener à bien la mise en œuvre?
Évaluation des risques	Comment le profil de risque de chaque option se compare-t-il?
Points de référence	Comment les options se comparent-elles aux normes de l'industrie ou aux points de référence des forces alliées?
Facteurs touchant les politiques et les normes	Comment se compare l'incidence des options sur les politiques et les normes du MDN et des FAC (p. ex., sécurité, protection des renseignements personnels, accessibilité, gestion de l'information et architecture d'entreprise)?

Dans l'ensemble, l'analyse des options sera axée sur la création des résultats attendus suivants :

a. l'analyse de rentabilisation, appuyée par un énoncé préliminaire des besoins élaboré en consultation avec les intervenants opérationnels et l'industrie, et par les données relatives aux coûts produites avec l'aide de l'industrie;

b. un plan détaillé du déroulement de la définition (les coûts aussi), y compris une Stratégie intégrée d'approvisionnement en matière de défense (SAMD) qui repose sur des données probantes et l'expérience acquise grâce à la mobilisation de l'industrie au cours de l'étape d'analyse des options;

c. un plan indicatif du déroulement de la mise en œuvre (y compris les coûts);

d. un plan indicatif du déroulement du soutien en service et de l'exploitation après la mise en œuvre (y compris les coûts).

Une fois ces travaux terminés, le projet sera soumis à l'examen, à l'appui et à l'approbation du Conseil

des capacités de la Défense (CCD), du Conseil de gestion du programme (CGP) du MDN, de la Commission indépendante d'examen des acquisitions de la Défense (CIEAD) et, finalement du Conseil du Trésor.

ANNEXE B : ENVIRONNEMENT DE MISSION ET SCÉNARIOS OPÉRATIONNELS

1 INTRODUCTION

1.1 Contexte

La politique de défense du Canada, *Protection, sécurité, engagement*, définit les missions principales des FAC et l'obligation pour les FAC d'exécuter des opérations simultanées.

La lettre de mandat du ministre de la Défense nationale exige également que les FAC, si on fait appel à elles, soient équipées et préparées pour protéger la souveraineté du Canada, défendre l'Amérique du Nord, aider en cas de sinistre, mener des missions de recherche et sauvetage, appuyer les opérations de paix des Nations Unies et contribuer à la sécurité de nos alliés, y compris dans le cadre d'opérations des forces alliées et de la coalition à l'étranger.

Pour remplir ces rôles, les FAC doivent être une force militaire moderne, efficace, agile, réactive, bien entraînée et bien équipée, dotée des capacités de base et de la souplesse nécessaires pour contrer avec succès les menaces conventionnelles et asymétriques, y compris le terrorisme, les insurrections et les cyberattaques. En outre, les FAC doivent disposer des capacités nécessaires pour apporter une contribution significative à l'ensemble des opérations, de l'aide humanitaire à la défense collective.

2 ENVIRONNEMENTS DE MISSION

2.1 Exigences relatives aux missions principales et opérations simultanées des FAC

La politique de défense du Canada, *Protection, sécurité, engagement*, précise les missions principales des FAC et les exigences relatives aux opérations simultanées (c.-à-d., les capacités de soutien aux missions que l'infrastructure informatique livrée doit fondamentalement être en mesure de soutenir).

2.1.1 Exigences visant les missions principales des FAC

- Détecter et dissuader les menaces ou les attaques visant le Canada et s'en défendre.
- Détecter et dissuader les menaces et les attaques visant l'Amérique du Nord et s'en défendre en partenariat avec les États-Unis, notamment par l'entremise du NORAD.
- Diriger des efforts de l'OTAN ou de coalitions visant à dissuader et à défaire des adversaires, y compris des terroristes, à l'appui de la stabilité mondiale ou contribuer des forces à ces efforts.
- Diriger des opérations de paix et des missions de stabilisation internationales avec les Nations Unies, l'OTAN et d'autres partenaires multilatéraux ou contribuer à celles-ci.
- Participer au renforcement des capacités à l'appui de la sécurité d'autres pays et de leur capacité à apporter une contribution à la sécurité à l'étranger.
- Prêter assistance aux autorités civiles et aux organismes d'application de la loi, y compris ceux chargés de la lutte contre le terrorisme, à l'appui de la sécurité nationale et de la sécurité des Canadiens à l'étranger.
- Prêter assistance aux autorités civiles et aux partenaires non gouvernementaux à la suite de catastrophes ou d'urgences majeures survenant au pays ou à l'étranger.
- Mener des opérations de recherche et de sauvetage.

2.1.2 Exigences visant les opérations simultanées des FAC

- Défendre le Canada, notamment en répondant simultanément à plusieurs urgences nationales á l'appui des autorités civiles.
- Respecter leurs obligations auprès du NORAD, notamment au moyen de nouvelles capacités dans certains domaines.
- Respecter leurs engagements auprès des alliés de l'OTAN en vertu de l'article 5 du Traité de l'Atlantique Nord.
- Apporter une contribution à la paix et la stabilité internationales en étant en mesure de mener:
    - deux déploiements prolongés d'environ 500 à 1 500 militaires, dont un en tant que pays chef de file;
    - un déploiement à durée limitée (6 à 9 mois) d'environ 500 à 1 500 militaires;
    - deux déploiements prolongés d'environ 100 à 500 militaires;
    - deux déploiements à durée limitée (6 à 9 mois) d'environ 100 à 500 militaires;
    - un déploiement de l'Équipe d'intervention en cas de catastrophe (EICC) comprenant du soutien supplémentaire adaptable; et
    - une opération d'évacuation de non-combattants comprenant du soutien supplémentaire adaptable.

2.2 Environnement opérationnel

2.2.1 Les commandants et le personnel dans l'ensemble du pays pourront accéder au réseau à partir d'une variété d'environnements, y compris les bureaux, les salles des opérations et les sites de déploiement, au moyen des postes de travail appropriés à l'environnement de travail de l'utilisateur (ordinateurs de bureau, terminaux clients légers, ordinateurs portatifs, ordinateurs portatifs robustes, etc.).

2.2.2 Les actifs en mer de la Marine royale du Canada (MRC) et les actifs en vol de l'Aviation royale du Canada (ARC) auront accès au réseau grâce à l'infrastructure de soutien de la MRC et de l'ARC, respectivement, ce qui permettra aux utilisateurs de ces environnements d'avoir accès au réseau. De même, les actifs du Commandement – Forces d'opérations spéciales du Canada (COMFOSCAN) seront reliés au moyen d'infrastructure unique, adaptée à leur emplacement et à leur mission.

2.2.3 Les centres de données pour l'infrastructure informatique à l'appui de C2 fonctionneront dans un environnement physique à ambiance contrôlé, dans un petit nombre d'emplacements clés.

2.2.4 Une infrastructure de réseautage sera installée dans tous les bâtiments où se trouvent des utilisateurs. Dans ces bâtiments, les locaux d'équipement (armoires de communication) seront chauffés, mais ne seront peut-être pas climatisés. En outre, la connectivité sera étendue aux quartiers généraux déployés, qui peuvent se trouver dans des structures temporaires, y compris des conteneurs maritimes, des véhicules (y compris des remorques) et des tentes, qui permettront une certaine protection contre les intempéries, y compris la climatisation.

2.2.5 Le personnel de soutien pourra accéder au réseau à partir d'emplacements régionaux de soutien, qui seront situés dans des bureaux. Ce personnel aidera également les utilisateurs, sur leurs lieux de travail, si nécessaire, et travaillera sur l'infrastructure de réseau où qu'elle se trouve. Certains membres du personnel de soutien seront présents aux sites de déploiement.

2.2.6 Le système fonctionnera dans un environnement cybernétique où les menaces de cyberattaques peuvent émaner à la fois de forces militaires asymétriques et conventionnelles. Ces menaces pourraient provenir d'États et de groupes indépendants et influer sur les opérations nationales et expéditionnaires. De plus, même si le réseau n'aura aucune connectivité directe à l'internet, il sera sujet à des cyberattaques d'origine externe qui ont migré dans le réseau classifié par le biais d'autres réseaux (p. ex., le réseau d'un allié ou d'un autre ministère). Il sera également vulnérable aux cyberattaques d'origine interne provenant d'utilisateurs mal intentionnés, qui utilisent une clé USB ou tout autre mécanisme de transfert de données.

2.2.7 La connectivité entre les sites reposera sur des dispositifs commerciaux. Ainsi, les réseaux classifiés dépendront de ces actifs de communication, qui sont vulnérables aux menaces physiques et virtuelles.

2.2.8 Les données de niveau Secret stockées sur le réseau seront une cible précieuse pour les attaques de l'adversaire. Elles procureraient des renseignements sur les capacités et la posture des FAC ainsi qu'un aperçu des connaissances du MDN et des FAC sur les activités, l'équipement et l'état de préparation de l'adversaire. Des renseignements détaillés sur la configuration et l'état des services informatiques et des biens informatiques au sein de l'infrastructure informatique constitueront également une cible précieuse pour les cyberattaques de l'adversaire.

ANNEXE C : ÉNONCÉ PRÉLIMINAIRE DES EXIGENCES

1 FONCTIONNEMENT GÉNÉRAL

1.1 Concept d'opération (CONOPS)

Le système permettra aux utilisateurs d'accéder en temps opportun et de façon sécuritaire et intégrée à tous les renseignements opérationnels et institutionnels dont ils ont besoin et pour lesquels ils détiennent l'autorisation. Il communiquera aussi avec les organismes gouvernementaux, les alliés et d'autres partenaires, et appuiera les services à fort débit de données comme la fusion des données et le ciblage. Cette mise à niveau reposera sur la mise en place d'une infrastructure informatique cohésive et intégrée de niveau Secret qui améliorera la connectivité pour faciliter le partage et l'échange de données, de vidéos et d'éléments multimédias ainsi que la téléphonie au sein du MDN et des FAC et avec nos partenaires. Les utilisateurs pourront échanger des renseignements pertinents, en temps quasi réel, à tous les niveaux de sécurité, du niveau Sans classification au niveau Très secret au sein du MDN et des FAC, et au niveau Secret avec le GC, les États-Unis, le Groupe des cinq et les partenaires de l'OTAN, au moyen des solutions automatisées d'échange d'information et des solutions interdomaines.

Ce système permettra aux commandants du MDN et des FAC d'exercer plus efficacement le C2, car ces commandants et leur personnel pourront colliger et traiter l'information provenant de sources très variées, planifier et prendre des décisions, de même que diriger, coordonner et contrôler les forces afin d'obtenir un avantage opérationnel par rapport aux adversaires.

L'utilisateur aura un accès simultané et en temps opportun à toute l'information qu'il est autorisé à consulter à partir d'un seul terminal, ce qui réduira considérablement le temps nécessaire pour trouver, obtenir, analyser et traiter l'information opérationnelle et situationnelle critique. Il sera également beaucoup plus efficace dans ses tâches, car il ne perdra pas de temps à se connecter à de multiples systèmes par divers dispositifs et à diverses infrastructures, et à chercher des données dans un grand nombre de référentiels. Au lieu de cela, il pourra se connecter une seule fois, entrer les données une seule fois, les partager avec tous et trouver facilement l'information dans un environnement d'information intégré.

Le système fournira des services de base (p. ex., courriel, clavardage, navigation internet, partage de fichiers, voix sur protocole internet, vidéoconférence sécurisée, services d'annuaire) et facilitera le cas échéant l'utilisation d'applications de C2 ainsi que d'autres applications. Il permettra à l'utilisateur d'accéder à l'information à partir de n'importe quel endroit durable ainsi que de se déconnecter et de se reconnecter au besoin s'il est en déplacement. Le système étendra également ces services aux déploiements opérationnels et aux missions dans le monde entier, tout en facilitant l'échange d'information avec le réseau spécialisé des missions. Il assurera également la connectivité aux actifs en mer grâce à l'infrastructure de soutien de la MRC, y compris les centres d'opérations navales, et aux actifs en vol grâce à l'infrastructure de soutien de l'ARC que l'on trouve sur les bases d'opérations principales. Pour ces actifs en mer et en vol, les services seront optimisés pour refléter les environnements à faible bande passante dans lesquels ces actifs fonctionnent.

La sécurité opérationnelle sera renforcée par la mise en œuvre d'un système de gestion à plusieurs facteurs de l'identité et des droits d'accès, qui tiendra lieu d'unique système pour contrôler l'accès des utilisateurs aux réseaux, aux applications et aux services dans les divers domaines. L'utilisation d'un seul justificatif d'identité et d'une seule authentification simplifiera et accélérera l'accès à l'environnement d'information de niveau Secret. De plus, la sécurité opérationnelle sera renforcée en augmentant la sécurité axée sur les données, car l'accès à l'information sera déterminé pour chaque élément d'information, ce qui réduira le risque d'accès non autorisé. Pour réaliser cela, un étiquetage précis et indélébile des données, par l'étiquetage des métadonnées, sera mis en œuvre pour garantir l'application des restrictions en matière de classification de sécurité, de diffusion, de manipulation et de communautés d'intérêts. Pour ce faire, l'utilisateur devra étiqueter et classer toutes les données dans le système au fur et à mesure de leur production et de leur stockage dans le référentiel.

L'utilisateur accédera au système d'une manière très fiable, car la capacité du système à se rétablir des

erreurs et des dommages, ou à s'y adapter, sera améliorée par l'implémentation de redondance pour les dispositifs essentiels de traitement, de réseautage et de stockage. De par sa conception, le système se dégradera de façon prédéterminée dans des conditions défavorables, conformément aux priorités des commandants, et pourra continuer à fournir des services informatiques pendant la perte de connectivité à son réseau fédérateur. Il s'adaptera dynamiquement et automatiquement à l'évolution des rôles, des environnements et des besoins des utilisateurs en matière de traitement, de réseautage et de stockage, y compris temporairement pendant les périodes de pointe.

De plus, le système permettra la connectivité à certaines organisations déployées au niveau opérationnel, tant au Canada qu'à l'étranger. Par exemple, il peut s'agir d'un quartier général de la FOI des FAC déployé dans le cadre d'une coalition au Moyen-Orient, d'un quartier général de la FOIR déployé pour fournir une aide en cas de catastrophe en Colombie-Britannique ou d'une frégate déployée dans le cadre de l'opération ARTEMIS en mer d'Arabie. Le système assurera la connectivité aux éléments canadiens déployés et aux réseaux connexes déployés pour appuyer les fonctions nationales de C2 du CEMD, du commandant du COIC et des commandants des contingents nationaux du Canada.

Pour les éléments déployés, le système procurera un accès aux services et aux sources d'information documentée hébergés sur les réseaux du MDN et des FAC, du GC, des États-Unis, comme le NORAD, du Groupe des cinq et de l'OTAN, qui ne sont pas accessibles depuis le réseau de la mission. Le système sera adaptatif, y compris les services de base, les serveurs appropriés de stockage, de traitement et d'application, en fonction de l'élément déployé. Le système déployé demeurera sur le théâtre des opérations pendant toute la durée de l'opération et pourra être augmenté ou réduit selon les besoins pendant toute la durée de la mission.

Le CONOPS détaillé sera élaboré au cours de l'étape de définition du projet, à mesure que sont définies la conception du système, les principales mesures de performance et les spécifications fonctionnelles. Il fera état des rôles et des responsabilités du personnel, des processus et procédures, ainsi que de leurs besoins en matière d'échange d'information.

1.2 Portée du projet

Inclus	Exclu
Mise en réseau des données militaires classifiées relatives au C2 ainsi qu'au commandement, au contrôle, aux communications, à l'informatique, au renseignement, à la surveillance et à la reconnaissance (C4ISR), y compris la téléphonie, les services multimédias et la vidéo, pour connecter les capteurs, les plateformes de capteurs, les communications et les actifs du réseau. Cela comprend les réseaux étendus (réseaux de communications noirs et rouges), les réseaux locaux et les services de téléphonie IP.	Services de transmission de données et de communications vocales non classifiés d'usage général et de niveau Très secret.
Connectivité réalisée au moyen de systèmes de communication par satellite, y compris l'acquisition d'une capacité supplémentaire, en tirant parti des services existants par satellite.	Acquisition de nouveaux systèmes de communication par satellite.
Passerelles d'information pour étendre le partage des données et de l'information à nos partenaires interarmées, interorganismes, multinationaux et publics. Cela inclut des solutions interdomaines visant à la fois les fonctions d'accès aux données et de transfert de données.	Fourniture ou acquisition de systèmes stratégiques de communication par radiofréquences.

Services classifiés d'espace de travail électronique et collaboratif, y compris le courriel, le clavardage et les services d'annuaire.	Développement ou amélioration des applications à l'appui des processus de C4ISR.
Services informatiques répartis, y compris le matériel client, les systèmes d'exploitation, les serveurs de fichiers et d'impression ainsi que les services d'accès à distance.	Acquisition de services ou d'appareils de connectivité mobile.
Services informatiques de production et d'exploitation, y compris les serveurs, la gestion des systèmes, la gestion des fonctions, la gestion des problèmes et des événements, la gestion des configurations et des changements, ainsi que les services de centres de données (y compris les solutions de stockage).	
Services de sécurité des données et de l'information, y compris l'étiquetage sécurisé et les services de sécurité axés sur les données.	
Services de sécurité informatique, y compris les services complets de gestion de l'identité et des droits d'accès, les services de sécurité du réseau et du périmètre, les antivirus et les services de chiffrement commercial.	
Soutien logistique intégré, y compris la formation, le soutien en service, les données techniques, etc.	

2 PRODUITS LIVRABLES GÉNÉRAUX

2.1 Les produits livrables du projet comprennent les suivants :

- Mise en œuvre de services de traitement, de stockage, de réseautage ainsi que d'espace de travail électronique et collaboratif modernisé, normalisé et durable, permettant l'accès à tous les services et à toute l'information à partir d'un point d'accès unique.
- Élimination des points de défaillance uniques par la redondance des services de traitement, de stockage et de réseautage, la diversité de l'accès local et la reprise après sinistre.
- Mise à niveau des fonctions actuelles de l'infrastructure informatique, notamment l'élargissement de la bande passante et l'augmentation de la base d'utilisateurs, mise en œuvre de la multidiffusion, du réseau sans fil, de l'accès basé sur l'utilisateur et le rôle, de fonctions d'optimisation du réseau et de continuité des activités ainsi qu'amélioration des services de sécurité des données et de l'information (y compris l'étiquetage des données et la gestion de l'identité et des droits d'accès).
- Réduction du nombre de réseaux de niveau Secret du MDN et des FAC par leur intégration en une seule infrastructure qui prend en charge à la fois les domaines Secret réservé au Canada et aux États-Unis (Secret CANUS) et Secret réservé aux Canadiens.
- Mise en œuvre d'un nouveau cadre de gestion des opérations et des services, notamment par la gestion des actifs, de la configuration, des versions et du déploiement, de la capacité, de la disponibilité, des incidents, des problèmes ainsi que de la surveillance et de l'exploitation du réseau.

- Mise en œuvre de l'accès simultané aux domaines de sécurité de niveau Secret et sans classification à partir d'un seul terminal.
- Mise en place de nouvelles passerelles d'échange de l'information d'entreprise et de solutions interdomaines pour accroître la capacité d'échange de données et d'information dans les domaines de sécurité au sein du MDN et des FAC ainsi qu'avec le GC, ses alliés et ses partenaires.
- Amélioration de l'intégration épisodique, en augmentant la capacité de lien arrière, en consolidant et en mettant à niveau les passerelles réseau et en mettant en œuvre des identités uniques.
- Mise en œuvre d'une fonction normalisée de quartier général épisodique modulaire, en éliminant les fonctions en double, et d'une trousse déployable normalisée de quartier général reposant sur une approche modulaire pour satisfaire aux exigences spécifiques de chaque chef d'état-major d'armée (CEMA).
- Définition d'une architecture commune d'entreprise pour prendre en charge l'intégration et l'évolution du système.
- Mise en œuvre d'une fonction complète de SLI.

2.2 Exigences préliminaires

Nota : Comme on ne fait pour ce projet que commencer à en définir les besoins, la liste suivante n'est ni complète ni confirmée. Entre autres, un certain nombre d'éléments de la liste doivent être confirmés : l'élément en question demeure ouvert à discussion avec les intervenants internes ainsi qu'aux commentaires et suggestions de l'industrie. Cela dit, la liste ci-jointe devrait donner à l'industrie une vue d'ensemble des fonctions que le projet vise à mettre en œuvre; en outre, il reste à établir à qui de l'industrie ou du gouvernement incombera la prestation de chacune des fonctions.

2.2.1 L'infrastructure informatique de niveau Secret doit comporter les fonctions de traitement, de réseautage et de stockage nécessaires pour satisfaire efficacement aux exigences des missions principales et des opérations simultanées de la Politique de défense du Canada – *Protection, sécurité, engagement* au moyen d'une infrastructure informatique normalisée, unifiée, stratégique et opérationnelle de C2 de niveau Secret.

2.2.1.1 Elle doit intégrer tous les réseaux de niveau Secret du MDN et des FAC (plus de 25) en une seule infrastructure.

2.2.1.2 Elle doit comporter les fonctions de traitement, de réseautage et de stockage nécessaires pour prendre en charge les utilisateurs devant avoir accès à la fois au niveau Secret réservé aux Canadiens et Secret CANUS.

2.2.1.3 Elle doit pouvoir prendre en charge au moins 25 000 utilisateurs.

2.2.1.4 Elle doit permettre aux utilisateurs d'accéder à toutes les données requises à partir d'un seul terminal.

2.2.1.5 Elle doit fournir aux utilisateurs une connexion unique à tous les services et domaines.

2.2.1.6 Elle doit comporter des fonctions de courriel.

2.2.1.7 Elle doit prendre en charge les données, la voix et la vidéo.

2.2.1.8 Elle doit comporter des fonctions de clavardage.

2.2.1.9 Elle doit comporter des fonctions de navigation internet.

2.2.1.10 Elle doit comporter des fonctions de partage de fichiers.

2.2.1.11 Elle doit comporter des fonctions de téléphonie IP.

2.2.1.12 Elle doit comporter des fonctions de vidéoconférence IP protégée en salle de conférence.

2.2.1.13 Elle doit comporter des fonctions de vidéoconférence IP protégée de bureau.

2.2.1.14 Elle doit comporter des centraux de services d'annuaire.

2.2.1.15 Elle doit comporter un système de gestion des ressources d'information (SGRI) ou être compatible avec l'ancien SGRI de l'IRSC.

2.2.1.16 La fonction de téléphonie IP de l'infrastructure doit fonctionner avec le Réseau de commutation rouge de la Défense canadienne (RCRDC) ou le remplacer, selon le cas. (Nota : Le RCRDC est un prolongement du RCRD américain incluant des fonctions sécurisées de voix et de téléconférence à plusieurs niveaux.)

2.2.1.17 L'infrastructure doit comporter des fonctions de vidéoconférence IP protégée haute définition en salle de conférence.

2.2.1.18 Les fonctions de vidéoconférence IP protégée haute définition en salle de conférence de l'infrastructure doivent pouvoir afficher simultanément au moins huit participants sur un seul écran. (à confirmer)

2.2.1.19 L'infrastructure doit être en mesure de fournir des fonctions de vidéoconférence IP protégée de bureau à tous les terminaux d'utilisateur.

2.2.1.20 Les fonctions de vidéoconférence IP protégée de bureau de l'infrastructure doivent pouvoir prendre en charge simultanément au moins huit participants. (à confirmer)

2.2.1.21 L'infrastructure doit prendre en charge les applications de C2 migrées à partir des infrastructures informatiques existantes de niveau Secret (p. ex., IRSC).

2.2.1.22 Elle doit prendre en charge les applications de C2 utilisées sur le Système de soutien du commandement de la Force terrestre (SSCFT) (ou son successeur) et le RCMD (ou son successeur).

2.2.1.23 Elle doit prendre en charge SharePoint et les autres outils de collaboration migrés à partir des infrastructures informatiques existantes de niveau Secret.

2.2.1.24 Elle doit comporter des fonctions d'archivage.

2.2.1.25 Elle doit comporter des fonctions partagées et sécurisées d'impression (au moins une imprimante par site et une par tranche de 100 employés – à confirmer).

2.2.1.26 Elle doit comporter des fonctions partagées de numérisation (au moins un numériseur par site et un par tranche de 100 employés – à confirmer).

2.2.1.27 Les données de l'infrastructure doivent être traitées et stockées au Canada ou, s'il y a lieu, dans des lieux sous contrôle canadien (p. ex., ambassade du Canada à l'étranger ou quartier général de théâtre).

2.2.1.28 L'infrastructure doit fonctionner 24 heures sur 24 et 7 jours sur 7.

2.2.1.29 Elle doit comprendre cinq (à confirmer) infrastructures déployables de traitement, de réseautage et de stockage en vue d'un déploiement et d'une utilisation sur le théâtre des opérations, chacune pouvant fonctionner de façon autonome en cas de perte de la fonction de lien arrière.

2.2.1.30 Elle doit pouvoir s'intégrer dans les 24 heures (à confirmer) au RCMD dans le cadre de nouveaux déploiements.

2.2.1.31 Elle doit prendre en charge la *NATO Core Metadata Specification* (NCMS).

2.2.1.32 Elle doit au besoin respecter toutes les spécifications relatives aux métadonnées approuvées par le MDN et les FAC qui s'ajoutent à la NCMS.

2.2.1.33 Elle doit prendre en charge une croissance annuelle de 30 % des fonctions de traitement, de réseautage et de stockage.

2.2.2 Elle doit assurer la connectivité des organisations opérationnelles et tactiques durables et épisodiques du MDN et des FAC.

2.2.2.1 Elle doit interconnecter tous les emplacements du MDN et des FAC à travers le Canada (évalués à plus de 400 emplacements de tailles diverses, dont certains peuvent se trouver dans un environnement géographique commun).

2.2.2.2 Sa connectivité doit exploiter au maximum les services existants de télécommunications de Services partagés Canada (SPC) ainsi que du MDN et des FAC.

2.2.2.3 Elle doit assurer la connectivité des systèmes stratégiques et opérationnels épisodiques déployés au Canada ou à l'étranger et leur fournir des services.

2.2.2.4 La connectivité de l'infrastructure visant les systèmes stratégiques et opérationnels épisodiques doit pouvoir utiliser les services de télécommunications gouvernementaux et commerciaux (précisés au cas par cas).

2.2.2.5 L'infrastructure doit assurer la connectivité des navires en mer (p. ex., frégates) par l'intermédiaire des systèmes de télécommunications de la MRC et leur fournir des services.

2.2.2.6 Elle doit assurer la connectivité des avions en vol (p. ex., Aurora) par l'entremise des systèmes de télécommunications de l'ARC et leur fournir des services.

2.2.2.7 Elle doit assurer la connectivité des établissements permanents et des délégations du MDN et des FAC situés à l'étranger (p. ex., le quartier général du NORAD, le quartier général de l'OTAN, l'État-major de liaison des Forces canadiennes (Washington) (ELFC(W)), etc.).

2.2.2.8 Elle doit assurer la connectivité avec les officiers et le personnel de liaison du MDN et des FAC situés au Canada et à l'étranger.

2.2.2.9 Elle doit assurer la connectivité des attachés militaires des FAC situés au Canada et à l'étranger.

2.2.2.10 Elle doit assurer la connectivité des organisations tactiques spécifiées (p. ex., SSCFT, Système d'information de l'état-major interarmées, etc.) et leur fournir des services.

2.2.2.11 La connectivité de l'infrastructure visant les organisations de niveau tactique doit pouvoir utiliser les services de télécommunications gouvernementaux et commerciaux (précisés au cas par cas).

2.2.2.12 L'infrastructure doit mettre en œuvre des interfaces communes pour toutes les fonctions de connectivité.

2.2.2.13 Ses services doivent prendre en charge les utilisateurs mobiles qui se connectent et se reconnectent au réseau.

2.2.2.14 Elle doit assurer la connectivité à l'infrastructure secrète du gouvernement du Canada (ISCG).

2.2.2.15 Elle doit assurer la connectivité à SIGNET (C5 ou version ultérieure).

2.2.2.16 Elle doit assurer la connectivité au SIPRNet des États-Unis (y compris le NORAD Enterprise Network (NEN)).

2.2.2.17 Elle doit assurer la connectivité au Secret Local Area Network (LAN) Internet/Joint Command and Control Support System du Royaume-Uni.

2.2.2.18 Elle doit assurer la connectivité au DSN/JCCS de l'Australie.

2.2.2.19 Elle doit assurer la connectivité au réseau étendu secret de la Nouvelle-Zélande.

2.2.2.20 Elle doit assurer la connectivité au réseau étendu NATO Secret (NSWAN).

2.2.2.21 Elle doit assurer la connectivité au système de recherche et d'exploitation de renseignement sur le champ de bataille (BICES) de l'OTAN.

2.2.2.22 Elle doit assurer la connectivité au moyen d'une bande passante suffisante pour répondre aux besoins des services de courriel.

2.2.2.23 Elle doit assurer la connectivité au moyen d'une bande passante suffisante pour répondre aux besoins des services de clavardage.

2.2.2.24 Elle doit assurer la connectivité au moyen d'une bande passante suffisante pour répondre aux besoins des services de navigation internet.

2.2.2.25 Elle doit assurer la connectivité au moyen d'une bande passante suffisante pour répondre aux besoins des services de partage de fichiers.

2.2.2.26 Elle doit assurer la connectivité au moyen d'une bande passante suffisante pour répondre aux besoins des services de téléphonie IP.

2.2.2.27 Elle doit assurer la connectivité au moyen d'une bande passante suffisante pour répondre aux besoins des services de vidéoconférence IP protégée en salle de conférence.

2.2.2.28 Elle doit assurer la connectivité au moyen d'une bande passante suffisante pour répondre aux besoins des services de vidéoconférence IP protégée de bureau.

2.2.2.29 Elle doit assurer la connectivité au moyen d'une bande passante suffisante pour répondre aux besoins des services d'annuaire centraux.

2.2.2.30 Sa fonction de téléphonie IP doit assurer la connectivité au RCRDC au moyen d'une bande passante suffisante, s'il n'est pas mis hors service.

2.2.2.31 L'infrastructure informatique de niveau Secret doit assurer la connectivité au moyen d'une bande passante suffisante pour répondre aux besoins des applications de C2 déterminées (p. ex., la fonction de gestion de l'espace de bataille interarmées).

2.2.2.32 Elle doit assurer la connectivité au moyen d'une bande passante suffisante pour répondre aux besoins de la Modernized Integrated Database (MIDB). (Nota : La MIDB est une base de données du renseignement militaire général.)

2.2.2.33 Elle doit assurer la connectivité au moyen d'une bande passante suffisante pour répondre aux besoins de SharePoint et d'autres services de collaboration.

2.2.2.34 Elle doit assurer la connectivité au moyen d'une bande passante suffisante pour soutenir l'échange de données brutes et traitées de capteurs entre les emplacements déterminés, y compris la vidéo en temps réel pleine vitesse (p. ex., bases principales d'opérations de l'ARC, centres d'opérations navales de la MRC, centres du renseignement, etc.).

2.2.2.35 Elle doit comporter des fonctions de QS qui peuvent assurer la satisfaction des exigences rigoureuses de performance du réseau définies pour les fonctions et les services pertinents, tels que les cibles acquises par le NORAD, les indications et les avertissements, ainsi que les fonctions de ciblage.

2.2.2.36 Elle doit assurer une connectivité durable à la station des Forces canadiennes (SFC) Alert (c.-à-d., par une liaison satellite et hyperfréquence).

2.2.2.37 Elle doit assurer la connectivité par le biais de multiples sauts satellites.

2.2.2.38 Elle doit assurer la connectivité aux organisations de services d'infrastructure informatique durables déterminées, y compris, sans s'y limiter, les terminaux de bureau et mobiles (p. ex., ordinateurs portatifs), les plateformes et les capteurs, les passerelles, les imprimantes, les serveurs et les centres de données.

2.2.2.39 Elle doit prendre en charge les protocoles IPv4 et IPv6.

2.2.2.40 Elle doit prendre en charge la multidiffusion et la radiodiffusion.

2.2.3 Elle doit permettre l'échange transparent et efficace de renseignements avec certains réseaux secrets de partenaires et entre les domaines de sécurité.

2.2.3.1 Elle doit utiliser une passerelle d'échange de l'information sécurisée pour échanger des données jusqu'au niveau Secret CANUS avec le SIPRNet des États-Unis (y compris le NEN).

2.2.3.2 Elle doit utiliser une passerelle d'échange de l'information sécurisée pour échanger des données jusqu'au niveau Secret FVEY avec le SLI/JC2SS du Royaume-Uni.

2.2.3.3 Elle doit utiliser une passerelle d'échange de l'information sécurisée pour échanger des données jusqu'au niveau Secret FVEY avec le DSN/JCCS de l'Australie.

2.2.3.4 Elle doit utiliser une passerelle d'échange de l'information sécurisée pour échanger des données jusqu'au niveau Secret FVEY avec le réseau étendu secret de la Nouvelle-Zélande.

2.2.3.5 Elle doit utiliser des solutions interdomaines sécurisées pour échanger des données jusqu'au niveau Secret réservé aux Canadiens avec l'ISGC et SIGNET (C5 ou version ultérieure).

2.2.3.6 Elle doit utiliser des solutions interdomaines sécurisées pour échanger des données jusqu'au niveau Secret OTAN avec le NSWAN et le BICES de l'OTAN.

2.2.3.7 Elle doit utiliser des solutions interdomaines sécurisées pour échanger de l'information non classifiée (c.-à-d., sans classification et Désigné) avec les infrastructures non classifiées du MDN et des FAC ainsi que celles du gouvernement.

2.2.3.8 Elle doit utiliser des solutions interdomaines sécurisées pour échanger des données jusqu'au niveau Secret réservé aux Canadiens avec l'infrastructure Très secret du MDN et des FAC.

2.2.3.9 La passerelle d'échange de l'information et les solutions interdomaines de l'infrastructure doivent être automatisées et ne nécessiter aucune interaction humaine pour réaliser toutes les transactions d'échange de données répondant à des critères d'approbation prédéfinis (p. ex., type de fichier, présence des étiquettes de confidentialité et de métadonnées générales requises, taille maximale, etc.).

2.2.3.10 Cette passerelle et les solutions connexes doivent saisir les transactions d'échange de données qui ne répondent pas aux critères d'approbation prédéfinis et générer une alerte système relative à l'action de consignation, alerte qui peut être transmise (p. ex., à un centre d'opérations) et enregistrée dans un journal système connexe.

2.2.3.11 Cette passerelle et les solutions connexes doivent avoir une latence maximale de données de 0,5 s (à confirmer) (pour les transactions d'échange de données approuvées).

2.2.3.12 Cette passerelle et les solutions connexes doivent prendre en charge les transactions d'échange de données générées par courriel, clavardage, navigation internet, partage de fichiers, téléphonie IP, services de vidéoconférence IP protégée en salle de conférence et de bureau ainsi que par centraux de services d'annuaire, applications de C2 précisées et autres fonctions précisées de soutien du C2 (p. ex., services de collaboration).

2.2.3.13 Cette passerelle et les solutions connexes doivent comporter une fonction qui permet d'empêcher le transfert de certains types de fichiers.

2.2.3.14 Cette passerelle doit remplacer les fonctions de l'ancienne passerelle d'échange de l'information PEGASUS ou être compatible avec ces fonctions, selon le cas.

2.2.3.15 Cette passerelle et les solutions connexes doivent effectuer la recherche de virus sur tous les fichiers transférés.

2.2.3.16 Cette passerelle et les solutions connexes doivent produire des enregistrements d'une piste de vérification de toutes les demandes de transfert de données et de leurs résultats.

2.2.4 L'infrastructure doit permettre aux utilisateurs du MDN et des FAC d'accéder simultanément à l'information résidant dans les domaines de niveau Secret (toutes les restrictions) et sans classification et d'afficher simultanément cette information à l'aide d'un seul poste de travail.

2.2.4.1 Elle doit permettre un accès sécurisé et simultané à un minimum de six (à confirmer) domaines différents et l'affichage de ces six domaines au moyen d'un seul terminal.

2.2.4.2 Elle doit permettre un accès sécurisé et simultané aux domaines de sécurité Secret réservé aux Canadiens, Secret CANUS et RED et l'affichage de ces domaines au moyen d'un seul terminal en guise de fonction de base.

2.2.4.3 Elle doit également (c.-à-d., en plus de la fonction de base) permettre l'accès sécurisé et simultané au NSWAN et l'affichage du NSWAN au moyen d'un seul terminal pour des utilisateurs précisés.

2.2.4.4 Elle doit également (c.-à-d., en plus de la fonction de base) permettre l'accès sécurisé et simultané au BICES et l'affichage du BICES au moyen d'un seul terminal pour des utilisateurs précisés.

2.2.4.5 Elle doit également (c.-à-d., en plus de la fonction de base) permettre l'accès sécurisé et simultané au BICES-X des États-Unis et l'affichage du BICES-X au moyen d'un seul terminal pour des utilisateurs précisés.

2.2.4.6 Le terminal (unique) de l'infrastructure doit afficher chaque domaine de sécurité dans des fenêtres subordonnées distinctes à l'intérieur d'une fenêtre principale.

2.2.4.7 Il doit permettre aux utilisateurs de redimensionner, de déplacer, de superposer, de minimiser et de maximiser les fenêtres subordonnées.

2.2.4.8 La fenêtre principale de ce terminal doit afficher dans des bannières en arrière-plan à la partie supérieure et à la partie inférieure les restrictions et le niveau de sécurité les plus stricts propres à l'ensemble des domains auxquels l'utilisateur accède simultanément, y compris lorsque certaines fenêtres subordonnées sont minimisées.

2.2.4.9 Les fenêtres subordonnées de l'infrastructure doivent afficher dans une bannière à la partie supérieure les restrictions et le niveau de sécurité qui lui sont propres.

2.2.4.10 L'infrastructure doit utiliser un seul câble ou lien de réseau pour connecter les terminaux d'utilisateur à l'infrastructure de réseau (c.-à-d., accepter plusieurs domaines de sécurité sur le même câble ou lien de réseau).

2.2.4.11 Elle doit utiliser des fonctions commerciales et approuvées de chiffrement pour une utilisation classifiée entre les terminaux d'utilisateur et l'infrastructure de réseau (p. ex., vers les commutateurs du RL).

2.2.5 Elle doit se rétablir des imprévus et des dommages par la redondance des principaux dispositifs, ou s'y adapter, et se dégrader gracieusement conformément aux priorités des commandants.

2.2.5.1 Elle doit avoir un taux de disponibilité de 99 999 % (à confirmer).

2.2.5.2 Elle doit avoir une moyenne de temps de bon fonctionnement (MTBF) de 30 jours (à confirmer).

2.2.5.3 Elle doit comporter des fonctions suffisantes de traitement, de réseautage (y compris les passerelles d'échange de l'information et les solutions interdomaines) et de stockage pour assurer la continuité des opérations de C2 du MDN et des FAC.

2.2.5.4 Ses fonctions redondantes doivent satisfaire aux exigences de séparation géographique précisées en matière de survie (à confirmer).

2.2.5.5 Elle doit protéger par blocs d'alimentation sans coupure tous les principaux serveurs de traitement et de stockage.

2.2.5.6 Elle doit assurer la synchronisation des données sur le réseau.

2.2.5.7 Elle doit comporter une fonction de sauvegarde et de récupération des données pour tous les serveurs de données.

2.2.5.8 Elle doit effectuer quotidiennement une sauvegarde des données de tous les serveurs de données.

2.2.5.9 Elle doit permettre la récupération des données sauvegardées au cours des 30 jours précédents en moins d'une heure durant les heures ouvrables et de trois heures en dehors des heures ouvrables (à confirmer).

2.2.5.10 Elle doit permettre la récupération des données de plus de 30 jours sauvegardées au cours de l'année précédente en un jour ouvrable (à confirmer).

2.2.5.11 Elle doit permettre la récupération des données sauvegardées antérieurement à l'année précédente dans un délai de trois jours ouvrables (à confirmer). (Nota : cette exigence ne s'applique pas aux données officiellement transférées à Bibliothèque et Archives Canada).

2.2.5.12 Elle doit permettre à des utilisateurs essentiels précisés de continuer à exécuter leurs tâches de C2 sur place après la perte de la connectivité nodale (c.- à-d., jusqu'au rétablissement de la connectivité).

2.2.5.13 Elle doit comporter des sites de reprise après sinistre pour les fonctions de base de C2.

2.2.6 Elle doit comporter des mesures de gestion centralisée des opérations et du cycle de vie des services reposant sur les pratiques exemplaires en matière de BITI, de même qu'assurer l'harmonisation en temps opportun des services informatiques avec les besoins opérationnels et institutionnels.

2.2.6.1 Elle doit comporter une fonction centralisée de gestion du changement pour appuyer les processus de gestion du changement.

2.2.6.2 Elle doit comporter une fonction centralisée de surveillance et de gestion de la configuration des actifs de service pour appuyer la transition des services.

2.2.6.3 Elle doit comporter une fonction centralisée de gestion des versions et des déploiements pour appuyer la transition des services.

2.2.6.4 Elle doit comporter une fonction centralisée de gestion des connaissances pour appuyer les processus de gestion des services informatiques.

2.2.6.5 Elle doit comporter une fonction centralisée de gestion des événements pour appuyer les opérations d'entretien et les fonctions connexes.

2.2.6.6 Elle doit comporter une fonction centralisée de gestion des incidents pour appuyer les opérations d'entretien et les fonctions connexes.

2.2.6.7 Elle doit comporter une fonction centralisée de gestion des problèmes pour appuyer les opérations d'entretien et les fonctions connexes.

2.2.6.8 Elle doit comporter une fonction centralisée de gestion du traitement des demandes afin d'appuyer les opérations d'entretien et les fonctions connexes.

2.2.6.9 Elle doit comporter une fonction centralisée de catalogage des services pour soutenir l'aspect de la conception des services du cycle de vie de la gestion des services et être en mesure de s'interfacer avec l'outil existant de gestion des services.

2.2.6.10 Elle doit comporter une fonction centralisée de planification de la capacité pour appuyer les processus de gestion des services informatiques.

2.2.6.11 Elle doit assurer une continuité centralisée des services informatiques pour appuyer l'aspect conception des services du cycle de vie de la gestion des services.

2.2.6.12 Elle doit comporter une fonction de bureau de service fonctionnant dans le cadre existant de gestion des services.

2.2.6.13 Elle doit permettre au personnel informatique d'administrer l'infrastructure à distance.

2.2.6.14 Elle doit permettre au personnel informatique d'administrer à distance les terminaux des utilisateurs sans fermer la session de l'utilisateur.

2.2.6.15 Elle doit permettre la mise à jour automatique des logiciels.

2.2.6.16 Elle doit permettre les mises à jour à distance des logiciels.

2.2.7 Elle doit s'adapter dynamiquement et automatiquement à l'évolution des rôles, des environnements, des fonctions et des besoins en matière de services.

2.2.7.1 Elle doit pouvoir surveiller en temps réel l'état des principaux dispositifs de traitement, de réseautage et de stockage.

2.2.7.2 Elle doit comporter une fonction de production en temps réel des alertes, des rapports et des dossiers de vérification sur l'état des principaux dispositifs de traitement, de réseautage et de stockage à l'intention du personnel gestionnaire du réseau.

2.2.7.3 Elle doit comporter une fonction d'harmonisation et de reconfiguration en temps quasi réel des principaux services de traitement, de réseautage et de stockage.

2.2.7.4 Elle doit comporter une fonction d'harmonisation et de reconfiguration des rôles des utilisateurs et des autres entités.

2.2.7.5 Elle doit pouvoir prendre en charge des pointes temporaires de traitement, de réseautage et de stockage d'un ordre maximal de 30 % (à confirmer) en temps quasi réel.

2.2.7.6 Elle ne doit pas subir de temps d'arrêt à la suite d'ajustements dynamiques à l'affectation et à la réaffectation des ressources de traitement, de réseautage et de stockage.

2.2.8 Elle doit permettre l'insertion de nouvelles fonctions sans influer sur d'autres sous-systèmes ou sans nécessiter une modification de la base de référence du système de l'infrastructure informatique.

2.2.8.1 Elle doit être conçue et mise en œuvre à l'aide des technologies informatiques les plus récentes et conformément aux dernières tendances informatiques (à la fin de la période de conception), dans le respect des autres contraintes liées aux exigences (p. ex., la sécurité).

2.2.8.2 Elle doit être conforme aux normes gouvernementales les plus récentes, sauf en cas de conflit avec les normes militaires requises pour satisfaire aux exigences de la mission de C2 des FAC.

2.2.8.3 Elle doit être conforme aux normes commerciales les plus récentes, sauf en cas de conflit avec les exigences militaires requises pour satisfaire aux exigences de la mission de C2 des FAC et aux normes gouvernementales.

2.2.8.4 Elle ne doit pas utiliser de technologies exclusives sur les dispositifs appartenant au MDN, sauf lorsque cela est jugé inévitable et expressément approuvé par le MDN.

2.2.8.5 Elle doit dans la mesure du possible utiliser un système modulaire, sauf lorsque cela est jugé inévitable et expressément approuvé par le MDN.

2.2.8.6 Elle doit utiliser des produits commerciaux, militaires et gouvernementaux disponibles sur le marché, sauf lorsque cela est jugé inévitable et expressément approuvé par le MDN.

2.2.8.7 Elle doit permettre l'ajout de nouvelles technologies dans les six mois (à confirmer) d'une demande faite par le MDN et les FAC.

2.2.8.8 Elle doit mettre en œuvre de nouveaux produits ainsi que de nouvelles technologies et fonctions en perturbant le moins possible le C2 des FAC et le fonctionnement de l'infrastructure.

2.2.8.9 Elle doit le cas échéant être mise à niveau technologiquement tous les quatre (4) ans (à confirmer).

2.2.9 Elle doit assurer et préserver la confidentialité, la disponibilité et l'intégrité des données.

2.2.9.1 Elle doit s'assurer que les renseignements de niveau Secret réservé aux Canadiens ne sont divulgués qu'aux citoyens canadiens et que les renseignements de niveau CANUS ne sont divulgués qu'aux citoyens canadiens et américains.

2.2.9.2 Elle doit être conforme aux politiques et aux normes de sécurité du MDN et du GC en matière de confidentialité, de disponibilité et d'intégrité (y compris les ententes pertinentes avec les partenaires alliés).

2.2.9.3 Elle doit avoir une autorisation d'exploitation obtenue du MDN et des FAC par le processus d'évaluation et d'autorisation de sécurité.

2.2.9.4 Elle doit comporter une fonction de GIDA.

2.2.9.5 Sa fonction de GIDA doit reposer sur une authentification approuvée à facteurs multiples par carte ICP.

2.2.9.6 L’infrastructure doit comporter une ICP approuvée qui assure l’intégrité, la confidentialité, l’identification et l’authentification des données, et comporter des fonctions de non-répudiation.

2.2.9.7 Elle doit comporter des fonctions d’autorisation de l’entité pour toutes les ressources ainsi qu’appliquer des contrôles de diffusion et des instructions de manipulation.

2.2.9.8 Elle doit soutenir la création et l’utilisation des communautés d’intérêts.

2.2.9.9 Elle doit appliquer le marquage de sécurité aux courriels et en soutenir l’utilisation.

2.2.9.10 Elle doit appliquer le marquage de sécurité aux messages de clavardage et en soutenir l’utilisation.

2.2.9.11 Elle doit appliquer le marquage de sécurité aux fenêtres de navigation internet et en soutenir l’utilisation.

2.2.9.12 Elle doit appliquer des étiquettes de confidentialité aux métadonnées de tous les fichiers et en soutenir l’utilisation.

2.2.9.13 Ses fonctions de numérisation doivent ajouter une étiquette de sécurité au document ainsi lu.

2.2.9.14 Les étiquettes de confidentialité de l’infrastructure doivent respecter les marques de sécurité et les formats définis dans les Ordonnances et directives de sécurité de la Défense nationale — Norme 6 : Normes de sécurité de l’information.

2.2.9.15 La fonction d’étiquetage des métadonnées confidentielles de l’infrastructure doit satisfaire aux exigences de la publication interalliée sur le traitement des données (ADatP) 4774 — Confidentiality Metadata Label Syntax de l’OTAN.

2.2.9.16 La fonction de l’infrastructure des métadonnées confidentielles doit satisfaire aux exigences de la publication interalliée sur le traitement des données (ADatP) 4778 — Metadata Binding Mechanism de l’OTAN.

2.2.9.17 L’infrastructure doit comporter des fonctions de cyberdéfense.

2.2.9.18 Elle doit comporter une fonction de détection et de protection qui repose sur la signature et le comportement des maliciels.

2.2.9.19 Elle doit prendre en charge les fonctions de vérification du MDN.

2.2.9.20 Elle doit comporter une fonction de création de rapports de vérification et de statistiques pour le MDN.

2.2.9.21 Elle doit permettre aux OSSI du MDN d’accéder au besoin à l’infrastructure dans l’exercice de leurs fonctions (p. ex., enquête sur les incidents de sécurité).

2.2.9.22 Elle doit comporter une fonction d’évaluation post-événement des incidents de sécurité.

2.2.9.23 Elle doit utiliser des clients légers comme terminal d’utilisateur de base, sauf indication contraire (p. ex., pour répondre à des besoins informatiques intensifs, comme le traitement intensif de données locales spécialisées).

2.2.9.24 Elle doit permettre au MDN et aux FAC de restreindre les autorisations des utilisateurs en matière d’utilisation des supports externes et d’impression.

2.2.9.25 Elle doit comporter une fonction de soutien logistique entièrement intégrée.

2.2.9.26 Elle doit comprendre le personnel nécessaire pour assurer le soutien en service (structure et composition du personnel de l’entrepreneur ou du MDN et des FAC à confirmer, selon la solution choisie).

2.2.9.27 Elle doit être livrée avec toutes les données et les publications techniques nécessaires à son exploitation et son soutien.

2.2.9.28 Elle doit comprendre les installations nécessaires à l’exploitation et au soutien du système.

2.2.9.29 Elle doit être livrée avec les composants de rechange nécessaires pour satisfaire aux exigences de disponibilité pendant les deux (2) premières années après la livraison (à confirmer).

2.2.9.30 Elle doit être livrée avec l'équipement de soutien et d'essai nécessaire par le personnel du MDN et des FAC pour exécuter les fonctions de soutien requises.

2.2.9.31 Les produits livrables de l'infrastructure doivent inclure les installations de développement de niveau sans classification et les installations de prédéploiement de niveau Secret pour permettre l'évaluation et la préintégration de nouvelles fonctions et technologies.

2.2.9.32 Elle doit être livrée avec une trousse de formation pour l'administrateur système.

2.2.9.33 Elle doit être livrée avec une trousse de formation sur l'exploitation et la maintenance.

2.2.9.34 Elle doit être livrée avec une trousse de formation sur le déploiement en théâtre à l'intention des officiers d'état-major du SCI des quartiers généraux opérationnels.

2.2.9.35 Elle doit être livrée avec une trousse de formation pour les utilisateurs de la direction.

2.2.9.36 Elle doit être livrée avec une trousse de formation avancée pour les utilisateurs (c.-à-d., pour fournir un soutien local à la communauté des utilisateurs cadres et des utilisateurs généraux si un soutien par bureau d'aide n'est pas justifié).

2.2.9.37 Elle doit être livrée avec une trousse de formation de base des utilisateurs.

2.2.9.38 Elle doit être livrée avec une séance de formation initiale d'administrateur système.

2.2.9.39 Elle doit comprendre une formation initiale sur l'exploitation et la maintenance pour le personnel informatique précisé.

2.2.9.40 Elle doit comprendre une formation initiale sur le déploiement sur le théâtre à l'intention de certains officiers d'état-major du SCI des quartiers généraux opérationnels.

2.2.9.41 Elle doit comprendre une formation initiale pour les utilisateurs du niveau de la direction à l'intention de certains cadres supérieurs.

2.2.9.42 Elle doit comprendre une formation initiale avancée pour le personnel précisé.

2.2.9.43 Elle doit comprendre une formation initiale de base pour le personnel précisé.

2.2.10 Elle doit rester sous le contrôle du MDN et des FAC.

2.2.10.1 Le MDN et les FAC doivent participer à toutes les étapes du cycle de vie du système (élaboration, conception, construction et gestion).

2.2.10.2 La livraison du système ou des fonctions ne doit pas avoir d'incidence sur les exigences fonctionnelles, opérationnelles, techniques et de sécurité définies par l'autorité du MDN et des FAC, sans l'approbation explicite et l'acceptation des risques connexes par cette autorité.

2.2.10.3 La livraison du système ou des fonctions doit être facilement transférable à une autre organisation de prestation de services au cas où l'organisation principale de prestation de services ne pourrait plus satisfaire aux exigences définies par l'autorité du MDN et des FAC.

2.3 Classification de sécurité

2.3.1 Les fonctions supportées par l'infrastructure informatique à l'appui du projet de C2 doivent être mises en œuvre conformément aux lignes directrices sur les évaluations et les autorisations de sécurité. Le processus complet devra être terminé avant la mise en œuvre, afin d'assurer la diffusion des directives appropriées sur la mise en œuvre du matériel, des logiciels, du personnel et des procédures nécessaires pour satisfaire aux exigences de sécurité des fonctions.

2.3.2 Toute mesure future d'approvisionnement prise à l'égard de l'infrastructure informatique à l'appui de la solution de C2 exigera que les fournisseurs soient inscrits au Programme des marchandises contrôlées, et pourrait nécessiter qu'ils détiennent une cote de sécurité de niveau II (Secret) et,

éventuellement, de niveau III (Très secret) délivrée par leur agence de sécurité nationale respective. Certains fournisseurs devront aussi satisfaire aux exigences du GC pour fournir des produits et des services visés par des restrictions relatives à des données réservées aux Canadiens (classifiées).

2.3.3 Les fournisseurs et leurs sous-traitants peuvent être tenus de se conformer à des ententes de non-divulgation ou à d'autres restrictions liées à la sécurité.

2.3.4 En raison des risques et des menaces liés aux fonctions de C2 des FAC, les nombreux dispositifs, sinon la plupart, acquis dans le cadre du présent projet devront provenir de fabricants dignes de confiance (c.-à-d., intégrité de la chaîne d'approvisionnement). En conséquence, les fournisseurs devront satisfaire à des exigences contractuelles afin d'assurer de manière appropriée l'intégrité, la disponibilité et la confidentialité des dispositifs et des services de l'infrastructure de C2 de niveau Secret des FAC, et d'atténuer les menaces et les vulnérabilités liées aux technologies potentiellement vulnérables ou modifiées. La section 6 des *Clauses contractuelles visant l'équipement et les services de télécommunications (TSCG-01\G)* fait état des clauses de sécurité qui peuvent être incluses dans les contrats de Services publics et Approvisionnement Canada (SPAC). Il importe de les consulter pour obtenir des éclaircissements sur les facteurs de sécurité liés à l'intégrité de la chaîne d'approvisionnement.

2.4 Disponibilité opérationnelle

2.4.1 La disponibilité opérationnelle variera d'élevé à très élevé, selon les dispositifs ou les éléments précis du système. Les détails seront fournis plus tard, après leur définition.

2.5 Fiabilité

2.5.1 La fiabilité variera d'élevé à très élevé, selon les dispositifs ou les éléments précis du système. Les détails seront fournis plus tard, après leur définition.

2.6 Durabilité de l'environnement

2.6.1 La fonction livrée doit répondre aux normes du MDN en matière d'intendance de l'environnement.

2.7 Santé et sécurité

2.7.1 La fonction livrée ne doit pas susciter chez les opérateurs des préoccupations en matière de santé ou de sécurité au-delà de celles imposées par l'environnement opérationnel.

2.7.2 La fonction livrée doit être conforme à tous les codes de santé et de sécurité du MDN et des FAC.

2.8 Exigences relatives à la livraison

2.8.1 Le MDN et les FAC doivent pouvoir exercer un contrôle autoritaire sur l'infrastructure informatique.

2.8.2 La migration vers la nouvelle infrastructure informatique ne doit pas avoir d'incidence sur la continuité du C2.

2.9 Exigences relatives au personnel et à la formation

2.9.1 Comme le système remplace une fonction existante du MDN et des FAC, qui continuera de soutenir les mêmes applications utilisées avant la mise en œuvre, les besoins en matière de formation des utilisateurs devraient être minimes. Le changement le plus important pour les utilisateurs touchera l'étiquetage des données. Cette tâche n'est actuellement pas requise aux niveaux Secret ou sans classification et imposera de nouvelles exigences aux utilisateurs. L'équipe de projet procédera à une évaluation des besoins en matière de formation afin de déterminer la formation nécessaire et le meilleur mode de prestation.

2.9.2 Pour les administrateurs de réseau, les besoins en matière de formation devront être déterminés, car les changements apportés à la configuration du système et aux outils de gestion ne seront pas clairement compris avant l'étape de mise en œuvre.

2.9.3 Les conseillers en environnement et en communications conjointes (N6/G6/A6/J6) peuvent avoir besoin d'une formation afin de comprendre les fonctions du nouveau système, d'être en mesure de planifier sa mise en œuvre et son déploiement ainsi que de fournir des conseils aux commandants et au personnel sur l'utilisation opérationnelle de la nouvelle infrastructure informatique.

ANNEXE D : RÉTROACTION DE L'INDUSTRIE

1 INTRODUCTION

1.1 Étant donné qu'une grande partie de l'information nécessaire pour procéder à une analyse approfondie et significative des options provient de l'industrie en général et que le succès du projet dépendra entièrement de la capacité de l'industrie d'appuyer et d'exécuter le projet d'une façon ou d'une autre, nous avons l'intention, dans le cadre du projet, de mobiliser et de consulter activement l'industrie tout au long des étapes de l'analyse des options et de définition pour élaborer une stratégie cohérente et efficace d'approvisionnement en matière de défense et ainsi assurer le succès de l'état final du projet.

1.2 Les commentaires de l'industrie aideront l'équipe de projet du MDN et des FAC à définir les éléments suivants :

a. l'énoncé des besoins d'une manière compréhensible pour l'industrie et significative pour le contexte opérationnel du MDN et des FAC, et ainsi contribuer à mieux décrire les besoins opérationnels;

b. « l'art du possible » en ce qui concerne les fonctions informatiques, les progrès au sein de l'industrie et la façon dont les grandes entreprises évoluent pour répondre à leurs besoins informatiques, ce qui conduit à une meilleure définition de l'énoncé des besoins, du budget et du calendrier nécessaires pour atteindre les objectifs du projet (à la fois technologiques, et industriels, approvisionnement);

c. l'incidence sur les personnes, les processus et la technologie des divers concepts proposés ainsi que les changements organisationnels qui seront nécessaires pour appuyer chaque solution conceptuelle;

d. la nature et les sources des coûts du projet, y compris la nécessité des tâches de l'étape de définition, les coûts de l'étape de la mise en œuvre et le soutien en service à long terme;

e. la stratégie d'approvisionnement la plus appropriée acceptable pour l'industrie afin de livrer le bon équipement au MDN et aux FAC en temps opportun, en mettant à profit les achats pour créer des emplois et favoriser la croissance, en plus de simplifier les processus d'approvisionnement.

2 RÉPONSE À LA LETTRE D'INTÉRÊT

2.1 L'industrie est invitée à répondre à cette lettre d'intérêt et à fournir les renseignements suivants au plus tard à la date et à l'heure de clôture précisée. Les répondants sont invités à tenir compte des éléments suivants dans leur réponse :

a. utilisez le format d'écriture de votre choix, mais indiquez les mêmes numéros de section, afin de faciliter l'analyse des réponses par le Canada.

b. il n'y a aucune limite au nombre de pages dans votre soumission; cependant, la longueur prévue ne devrait pas dépasser les 30 pages recto en format d'affaires standard;

c. si la taille du document ne dépasse pas six mégaoctets, vous pouvez soumettre votre réponse en format PDF non protégé (c.-à-d., sans mot de passe) par courriel à TPSGC.PADivisionQE-APQEDivision.PWGSC@tpsgc-pwgsc.gc.ca, sinon, on vous demande d'enregistrer une copie de votre document PDF (2003 ou plus récent) sur chacune de deux clés USB et de les envoyer par la poste à l'agent de négociation des marchés indiqué à la section 2.7 de la demande de soumissions;

d. la mise en forme de la soumission doit devrait préférablement suivre le format proposé ci-dessous :

1) section 1 : sommaire — 1 à 2 pages, résumant la soumission globale;

2) section 2 : profil de l'entreprise :

a) désignez une personne-ressource principale pour le répondant;

b) donnez une brève introduction et une description des capacités de l'entreprise, en soulignant les produits, les services et les capacités basées au Canada ainsi que l'expérience dans la prestation de solutions pertinentes aux objectifs du projet;

c) décrivez l'intention d'être le principal intégrateur de systèmes, un sous-traitant potentiel ou un fournisseur de produits ou services;

d) décrivez le cas échéant les partenariats établis avec d'autres industries qui seraient profitables pour la définition des exigences relatives aux fonctions du projet;

e) décrivez les principales hypothèses, contraintes, préoccupations, conclusions et recommandations dont, selon le répondant, le Canada devrait tenir compte afin que le projet évalue les différentes options;

3) section 3 : historique de l'entreprise :

a) propriété — indiquez si l'entreprise est de propriété canadienne ou étrangère;

b) entreprise :

i taille,

ii nombre d'employés,

iii revenus annuels;

c) clients;

d) structure :

i L'entreprise relève-t-elle d'une entreprise mère?

ii L'entreprise a-t-elle des filiales?

e) historique :

i Combien d'années d'expérience votre entreprise possède-t-elle dans la fourniture de solutions de gestion de l'information et de technologie de l'information (GI-TI) pour un réseau complexe?

ii Combien d'années d'expérience votre entreprise possède-t-elle en matière de partenariat pour offrir une solution de GI-TI?

f) lieux :

i Où se trouvent les succursales?

ii Où se trouve le siège social?

g) certifications — quelles certifications l'entreprise détient-elle? Organisation internationale de normalisation (ISO) 9001, Six Sigma, Modèle intégré d'évolution des capacités (CMMI), etc.;

h) cote de sécurité :

i. Quelles sont les cotes de sécurité des employés? Combien d'employés ont une cote de sécurité de niveau II (Secret)? De niveau III (Très secret)?

ii. Quel est le niveau de sécurité des documents que l'entreprise peut posséder?

iii. Si l'entreprise ou les employés n'ont pas de cotes de sécurité valables, l'entreprise ou les employés accepteraient-ils de se soumettre au processus d'autorisation de sécurité (personnel et documents)?

4) Section 4 : Observations et conseils – Vous devez :

a) formuler commentaires, remarques et conseils sur tout aspect de la présente lettre d'intérêt, y compris toute préoccupation qui pourrait aider à formuler une recommandation en vue de l'amélioration;

b) préciser les qualifications minimales que vous jugez nécessaires à toute entreprise pour participer à un tel projet.

ANNEXE E — ACRONYMES

Acronyme	Nom complet
ARC	Aviation royale canadienne
BICES	Système de recherche et d'exploitation de renseignement sur le champ de bataille
BITI	Bibliothèque de l'infrastructure des technologies de l'information
C2	Commandement et contrôle
C4ISR	Commandement, contrôle, communications, informatique, renseignement, surveillance et reconnaissance
CANUS	Canada-États-Unis
CCD	Conseil des capacités de la Défense
CEMA	Chef d'état-major d'armée
CEMD	Chef d'état-major de la Défense
CGP	Conseil de gestion du programme
CIEAD	Commission indépendante d'examen des acquisitions de la Défense
CIGEB	Capacité interarmées de gestion de l'espace de bataille
CMMI	Modèle intégré d'évolution des capacités
COIC	Commandement des opérations interarmées du Canada
COMFOSCAN	Commandement — Forces d'opérations spéciales du Canada
CONOPS	Concept des opérations
CST	Centre de sécurité des télécommunications
EICC	Équipe d'intervention en cas de catastrophe
ELFC(W)	État-major de liaison des Forces canadiennes (Washington)
FAC	Forces armées canadiennes
FOI	Force opérationnelle interarmées
FOIR	Force opérationnelle interarmées régionale
FVEY	Groupe des cinq
GC	Gouvernement du Canada
GIDA	Gestion de l'identité et des droits d'accès
GI-TI	Gestion de l'information et technologie de l'information
IaaS	Infrastructure-service
ICP	Infrastructure à clés publiques
IP	Protocole internet
IRSC	Infrastructure du réseau secret consolidé
ISGC	Infrastructure secrète du gouvernement du Canada
ISO	Organisation internationale de normalisation
ITaaS	Technologie de l'information-service
Mbit/s	Mégabits à la seconde
MDN	Ministère de la Défense nationale
MIDB	Modernized Integrated Database (États-Unis)
MPE	Mission Partner Environment (États-Unis)
MRC	Marine royale canadienne
MTBF	Moyenne des temps de bon fonctionnement
NCMS	NATO Core Metadata Standard
NEN	NORAD Enterprise Network
NORAD	Commandement de la défense aérospatiale de l'Amérique du Nord
NSA	National Security Agency (États-Unis)
NSWAN	NATO Secret Wide Area Network
NZ	Nouvelle-Zélande
OTAN	Organisation du traité de l'Atlantique Nord

PaaS	Plateforme-service
QS	Qualité du service
RCMD	Réseau canadien des missions déployées
RCRDC	Réseau de commutation rouge de la Défense canadienne
RED	Réseau étendu de la Défense
SAMD	Stratégie d'approvisionnement en matière de défense
SFC	Station des Forces canadiennes
SGRI	Système de gestion des ressources d'information
SID	Solution interdomaines
SLI	Soutien logistique intégré
SLI/JC2SS	Secret LAN Internet/Joint Command and Control Support System (Royaume-Uni)
SPAC	Services publics et Approvisionnement Canada
SPC	Services partagés Canada
SSCFT	Système de soutien du commandement de la Force terrestre
VFR	Virtualisation des fonctions de réseau
VoIP	Voix sur internet